Vidi

Recordable DVD Protection System

Broadcast Flag Certification

March 1, 2004

PHILIPS

hp invent

PHILIPS

Philips Electronics

March 1, 2004

Federal Communications Commission
Office of the Secretary
Att: Broadcast Flag Certifications
c/o Natek, Inc.
236 Massachusetts Avenue, N.E.
Suite 110
Washington, D.C. 20002

Re: **Vidi Recordable DVD Protection System**

Dear Ms. Dortch:

Philips Electronics North America Corporation ("Philips") and Hewlett-Packard Company ("HP") jointly submit for the Commission's consideration, the Vidi Recordable DVD Protection System ("Vidi"), and urge its approval by the Commission for use in conjunction with the "Broadcast Flag." Vidi is an encryption-based digital broadcast content protection technology that prohibits the indiscriminate redistribution of digital broadcast content that has been recorded onto removable media, specifically Digital Versatile Discs (DVDs) in the DVD+RW and DVD+R formats.

The attached "Broadcast Flag Certification" includes a general description of Vidi and how it works (including its scope of redistribution); a detailed analysis of the level of protection Vidi affords digital broadcast content; information regarding Vidi's acceptance among content owners, broadcasters, and hardware and software manufacturers; and a summary of the terms and conditions under which Vidi will be made available. Included as appendices are the Vidi technical specification (Appendix A) and the Vidi Content Protection Agreement (Appendix B).

PHILIPS
Philips Electronics North America Corporation
Franklin Square
1300 I Street N.W. Suite 1070 East
Washington DC 20005
www.philips.com
Tel: (202) 962-8550
Fax: (202) 962-8560

In accordance with Public Notice DA 04-145 (January 23, 2004), please find attached an original and four copies of this document. As required, an additional copy also is being delivered (to the FCC's headquarters) to the attention of the Commission's Media Bureau Chief, W. Kenneth Ferree. Please direct any questions concerning this matter to the undersigned.

Respectfully Submitted,

Thomas B. Patton
Vice President, Government Relations
Philips Electronics North America Corporation

David G. Isaacs
Director, Government and Public Policy
Hewlett-Packard Company

Enclosures: Vidi Broadcast Flag Certification (1 original and 4 copies)

cc (with enclosure): W. Kenneth Ferree, Chief, Media Bureau
William H. Johnson, Deputy Chief, Media Bureau
Rick Chessen, Associate Chief, Media Bureau
Susan Mort, Attorney Advisor, Media Bureau
John Wong, Chief, Engineering Division, Media Bureau

TABLE OF CONTENTS

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

1 Executive Summary

Philips Electronics North America Corporation (Philips) and Hewlett-Packard Company (HP) submit to the Commission their joint technology certification ("Broadcast Flag Certification") for the Vidi Recordable DVD Protection System (Vidi). This Broadcast Flag Certification is filed in accordance with the Commission's Report and Order establishing digital broadcast content protection requirements designed to protect against the indiscriminate redistribution of digital broadcast content over the Internet.

Vidi is a new content protection system, and Philips and HP are confident in its widespread adoption. Philips and HP will defer introducing the technology to market, and licensing the technology, until such time as the FCC issues its approval for Vidi for use with the Broadcast Flag.

Philips and HP are pleased that a number of key industrial partners have endorsed Vidi, including: Ricoh Company, Ltd; Yamaha Corporation; and Ahead Software AG.

Vidi

Vidi is an encryption-based technology that prohibits the indiscriminate redistribution of digital broadcast content that has been recorded onto removable media, specifically Digital Versatile Discs (DVD) in both DVD+RW and DVD+R formats. Vidi does so by ensuring that removable media containing Vidi-protected content can be played only by Vidi-compliant devices (CE and PC), none of which will redistribute content indiscriminately. In addition, a Vidi-compliant device will output digital forms of the protected content played from a Vidi DVD only using approved output technologies, none of which will redistribute content indiscriminately over the Internet. Finally, the Vidi system of protection resides in not only the hardware – CE and PC devices – but in the removable media and software application as well. This ensures that, in terms of security and renewability, Vidi cannot be compromised merely by an attack on one component of the system, and that the effectiveness of the system can be continually renewed.

Vidi is a robust, highly capable encryption-based technology designed to protect digital broadcast content from unauthorized Internet redistribution, while maintaining the vitally important qualities of innovation and competition in the marketplace that will ensure the success of the content protection. Most importantly, Vidi embraces the compatible goals of protecting digital broadcast content from unauthorized redistribution, while also ensuring consumers may continue to use their existing consumer electronics and personal computing hardware products. Consumers purchasing new Vidi-equipped devices – both CE and PC-based devices – will continue to exercise their preferences for how they lawfully use digital broadcast content in conformity with their longstanding expectations.

Vidi Incorporates the FCC's Functional Criteria

Vidi prevents the indiscriminate redistribution of digital broadcast content over the Internet by fully and faithfully achieving the functional criteria established by the Commission in its interim Broadcast Flag-compliant approval process for covered demodulator products, both for CE and PC devices.

- Vidi is secure, and will frustrate the efforts of ordinary users from defeating its protections using generally available tools or equipment.
- Vidi adheres to the scope of redistribution required under the Commission's interim rules, in that it concentrates fully on one element of today's digital entertainment and media environment in a consumer's home: removable media. By encrypting protected content so that it can only be read by compliant devices and ensuring that Vidi DVDs will only transmit that content through approved digital outputs, Vidi ensures that removable media maintains its role in the "chain of custody" that ensures a secure digital environment.
- Vidi incorporates concrete means of authenticating devices to ensure they are legitimately part of the Vidi system of protection, including individual authentication processes addressing the unique physical properties of closed CE and open PC devices.
- By placing Vidi in devices and media and in PC software, the system can confront and thwart attacks on recording and playback devices. In the event the cryptographic secrets in a device or software are compromised, the encryption keys included in the Vidi discs will be amended to exclude the keys associated with the compromised device. This ensures that compromised devices are revoked, while preserving the use of compliant devices by innocent parties, thus providing a concrete, reliable means of revocation of compromised devices.

Vidi strives to protect only one element, removable media, in the chain of custody of systems that make up today's entertainment and media environment in a consumer home. As such, Vidi is interoperable with any and all other approved technologies governing the other component parts of the digital entertainment and media environment in the home.

Vidi Preserves Consumer Expectations for Use and Enjoyment of DTV

Protecting digital broadcast content from indiscriminate redistribution has been identified by the Commission as a fundamental aspect of advancing the transition to digital television. The Commission also has identified consumers' use and enjoyment of DTV broadcasts as fundamental to the transition, and Philips and HP are pleased to propose a technology, in Vidi, that fully embraces consumer use and enjoyment of digital television content.

Consumers expect that, in purchasing new devices, their existing content libraries will not be rendered obsolete and that their legacy equipment will retain its full functionality. Vidi meets consumer expectations in the evolving digital media marketplace by ensuring that consumers may use their existing DVDs on new Vidi-compliant devices, and that content recorded on a Vidi device that is not restricted by the broadcast flag is playable on legacy devices.

Consumers have also come to expect that they may readily record broadcast programming for later viewing. Vidi will in no way interfere with consumers' ability to record digital broadcast programming easily, yet faithfully adhere to the Commission's policy of prohibiting the indiscriminate redistribution of digital broadcast content.

Vidi Will Be Made Available on a Reasonable and Nondiscriminatory Basis on Terms that Protect Competition and Innovation

Vidi will be made available on a reasonable and nondiscriminatory basis, as required by the Commission's Report and Order. Vidi licensing will be transparent, consistent from one licensee to the next, and includes a most favored nation provision ensuring that all licensees benefit from the same favorable terms. The agreement includes strong enforcement provisions, including both liquidated damages and third party beneficiary rights for content participants. The fees charged are generally below those charged for other content protection systems.

The Vidi agreement contains provisions designed to protect competition in the development of content protection technology and devices. It avoids first-mover advantage by permitting only very limited changes and by requiring an open process that includes both content participants and implementers. Implementers are not required to sign away their own intellectual property without compensation under a reciprocal non-assert. Further, the compliance rules applicable to broadcast DTV content are modeled closely after the rules applicable to Covered Demodulator Products directly subject to the FCC's own regulation, thus providing a consistent level of content protection throughout the system and ensuring that *all* FCC approved output and recording protection technologies can be used by a Vidi product.

2 Policy Framework: Protecting Digital Broadcast Content From Indiscriminate Redistribution Over The Internet

2.1 Description of The Problem Being Addressed

The Federal Communications Commission has adopted a regulation requiring the application of technological protection measures to prevent indiscriminate redistribution of digital broadcast television content over the Internet. At the same time, the Commission is considering the regulatory structure applicable to cable navigation devices, with a goal toward providing both redistribution control and, in appropriate cases, copy limitations. The current regulatory models used in both proceedings are most readily based on the application of encryption to digital recordings and digital outputs and the regulation of the handling of content by devices that encrypt the content (*e.g.,* playback devices).

Certain recording formats, most notably the DVD+R/+RW format, are not easily adaptable to existing encryption technologies. Further, there is a substantial need for competing technologies to ensure that the contracts on which technologies are offered remain reasonable and pro-consumer. Vidi offers encryption-based technological protection that (i) fits readily within the FCC's digital broadcast content protection regulatory regime, (ii) works comfortably with DVD+R/+RW recorders, (iii) protects content provider, manufacturer and consumer interests, and (iv) provides needed competition in digital broadcast content protection technology.

2.2 The "Chain of Custody" Encryption Model

One method for protecting digital content involves encryption of the content under a regime that prevents indiscriminate redistribution and imposes copy limitations in certain contexts (e.g., pay TV and basic cable). Protection of this kind is based on many devices cooperating in an unbroken "chain of custody" beginning at the moment the content arrives in the consumer's home and continuing throughout his or her viewing and recording of the content. Thus, the chain involves protection (either by encryption, physical barrier or other method) when the content is:

1. In transit within a device;
2. In-transit between devices;
3. Stored on removable media, *e.g.,* recordable DVDs; and
4. Stored on non-removable media, *e.g.*, a magnetic hard drive.

When a device receives encrypted content (either from an input or by playing back a recorded medium) it is required, as a condition of the right to decrypt, to protect that content, in turn, by limiting the outputs to which the content can be sent and the removable media on which the content may be recorded.

As described below, the Vidi Recordable DVD Protection System ("Vidi") seeks only to address one (critical) part of the chain: *storage of protected content on removable media, and specifically recordable DVDs using the DVD+RW and DVD+R formats.*

2.3 Protection of Video Content Stored on Recordable DVDs

Digital Versatile Discs (DVDs) are an optical storage media format that is commonly used for the recording and playback of audiovisual content.

A recordable DVD is a DVD onto which the consumer may store (or "write" or "burn") video or other data content using a DVD recorder. The DVD recorder, while still relatively new to the consumer electronics market, is expected to replace the VCR as the preferred consumer recording device, and already has become a widely available feature on new PCs. In this regard, the recordable DVD and DVD recording device represent a significant technology "bridge" between the consumer electronics and computing platforms.

Currently, three different standards exist for recordable DVDs: DVD-RAM, DVD-R/-RW and DVD+R/+RW.[1] Discs using the DVD-R/-RW and DVD+R/+RW standards are, to a great extent, compatible with existing DVD players; in other words, under ordinary conditions, a recording made on a DVD-R/-RW or DVD+R/+RW recorder will play on a legacy DVD player. The DVD-RW and DVD+RW designations refer to discs that are "re-writable" and may written and over-written repeatedly. The DVD-R and DVD+R designations refer to discs that may be written only once, and that in general provide a greater level of backward compatibility.

Because DVDs are easily portable and may be played on existing DVD players and drives, unencrypted recordings may be played back, output digitally and directed to the Internet without limitation. Thus, assuming adequate bandwidth were to become available, indiscriminate redistribution by a user could occur.

[1] The latter two are referred to, respectively, as "DVD-DASH-RW" and "DVD-PLUS-RW."

3 General Description of The Vidi Recordable DVD Protection System

3.1 What Is Vidi?

The Vidi Recordable DVD Protection System ("Vidi") is a method for preventing unauthorized redistribution of digital broadcast video content that is recorded on DVD+RW or DVD+R discs. The Vidi specification defines a system, based on proven cryptographic methods, to prevent indiscriminate redistribution over the Internet by encrypting recorded content on portable discs and ensuring that when played back, the content is only allowed to be transmitted over digital outputs that, in turn, protect the content in accordance with applicable regulatory and licensing requirements. The Vidi protection features are triggered when digital broadcast video content marked with the ATSC broadcast flag descriptor or with a "redistribution control" descriptor such as "EPN" used by certain other technologies is received by a video recorder that implements Vidi.[2] These redistribution control descriptors indicate when digital broadcast video content are subject to limitations on redistribution. Redistribution control is achieved by encrypting the recorded digital broadcast content and cryptographically binding the encrypted video to the physical media. Encryption of the content on the removable DVD disc by Vidi prevents non-compliant players from accessing the content, since, without the keys, encrypted video is indecipherable and of no value even if it is redistributed. Compliant playback devices are, in turn, subject to contractual compliance and robustness obligations that parallel the rules imposed by the FCC on "Covered Demodulator Products" with respect to Marked Content.

While the Vidi system protects content on removable media, it has little effect on content in other forms. Those aspects of protection under an encryption regime must be accomplished by other technologies or data handling requirements. However, a Vidi-compliant playback device will protect content stored internally under robustness rules and, as required for any broadcast flag-compliant device, will only be permitted to release that content over digital outputs protected by digital broadcast content protection technologies approved by the FCC.

3.2 How Does Vidi Work?

The Vidi system defines a method for protecting video content recorded on a DVD disc compliant with the DVD+RW standard. To function, the Vidi system requires the use of a new type of blank DVD+RW or DVD+R media ("Vidi DVD"). The Vidi DVD includes a Disc Key Block ("DKB") containing keys used to authenticate any Vidi-

[2] Vidi will also protect recordings of content marked as Copy One Generation to a level and subject to rules comparable to those provided under the DFAST license, and will refuse to make recordings of content marked Copy Never or Copy No More. However, these types of protection are irrelevant in the Broadcast Flag context. Philips and HP expect to seek approval for Vidi for use with cable and satellite content in connection with the Commission's Plug & Play proceeding.

compliant device or Vidi-compliant player/recorder software. Only Vidi drives and Vidi software applications will be able to use Vidi DVDs to record or play protected copies of digital broadcast video content – Vidi drives and Vidi software applications will refuse to make recordings of marked digital broadcast video content on non-Vidi blank media. Importantly, legacy DVD+RW recorders will be able to use Vidi DVDs for non-protected recordings, thus preserving the use of existing consumer equipment to the greatest extent possible.

Use of Encryption and Data-Binding. Vidi protects content through the encryption of video data using proven cryptographic methods, specifically using the Advanced Encrypted Standard (AES) cipher with a 128-bit key. Each sector of protected video data is encrypted using a sector key based on information specific to that sector for added security. For convenient navigation of an encrypted video recording, the beginning of every sector containing video content is not encrypted, thus allowing features expected by the user, such as fast forward and rewind, while still maintaining protection of the content. Because content encrypted with Vidi cannot be played on a legacy DVD player (including, especially, a PC-based DVD drive), the system is able to thwart indiscriminant redistribution of otherwise protected digital broadcast content over the Internet.

However, encryption of the video content is not, by itself, sufficient to prevent indiscriminate redistribution over the Internet. In order to prevent the wholesale transfer of the encrypted video, each Vidi recorder cryptographically binds the encrypted video data to the physical media of the individual Vidi DVD upon which it is stored. By so doing, playback of the content stored on the Vidi DVD can occur only if the protected video data is read from the same disc used for the original recording.

Response to Attacks. Using a carefully crafted procedure designed to prevent wrongful revocation, it may be determined that revocation of a specific compromised device is necessary and warranted. In such a case, all manufacturers of blank Vidi DVDs will be required to use a new version of the Vidi DKB – which simply no longer includes the revoked device's keys – on all future blank Vidi DVDs, thus rendering the compromised device useless for purposes of recording content on new Vidi DVDs. Additionally, new versions of PC software will be required to use a newer Application Key Block,[3] which will prevent authentication of individual PC drive keys.

3.2.1 Authentication

As with any system that uses cryptography to protect information, it is essential that communication of content only occur with devices that are a legitimate part of the system and not with hardware or software masquerading as compliant components. Authentication is the process by which a device is verified as being a legitimate part of the system. Vidi authenticates each device and software by means of a system of secret keys that are stored in the DKB, which is distributed on every blank Vidi DVD. Each Vidi DVD has a Root Key KR, which is concealed in the DKB using keys from every

[3] The Application Key Block AKB is a key block that is embedded in an application for the purpose of authenticating a device.

compliant device or software application.[4] The Root Key KR represents admission for a device into the Vidi system.

Only compliant devices will be able to obtain the Root Key KR from the DKB, and thus accept, store and playback protected content. Devices which have been revoked will not be able to obtain the Root Key KR from the DKB and as a result will not be able to accept, store and playback protected content. Each Vidi-enabled Player/Recorder contains a set of keys (called Node Keys) and a Device ID. The set of Node Keys are either unique to a physical Player/Recorder, or common to a single version of software.[5] When a recording or playback operation begins, the Vidi device uses its Device ID associated with its key set to locate the portion of the DKB containing the concealed KR for that particular device. Once the correct version of the concealed KR is found, one of the keys from the Node Key Set can produce the KR for that disc. With the KR in hand, protected Vidi recordings can be created and played back. If the DKB does not contain a version of KR for that device (such as in the case where the device or software has been compromised), then the device is revoked and can no longer access protected content from that disc.

In a closed device, authentication takes place between a Vidi DVD and the device itself – there is no opportunity to "listen in" on the conversation, nor is there an ability to insert incorrect information into the authentication process. Devices with open architectures, such as computers, are another matter and require a somewhat different approach. In that case, communication between a computer drive and compliant Vidi software is protected by a method using a second system of authentication, which is described in section 4.10 below.

3.2.1.1 Advantages of the DKB Authentication System

An essential property of any mass-market security system is that no single failure compromises the entire system. Vidi limits any failure that may occur so that the overall goal of preventing the widespread indiscriminate redistribution of content is still fulfilled. At the same time, ordinary users should not be inconvenienced when using the system for typical uses, nor should security updates obsolete consumer devices or media, lest consumers seek to subvert the system simply to retain expected functionality.

The following advantages are obtained by the Vidi DKB system:

Compromised devices (or software) will quickly find that new blank media are unavailable for use with these devices, rendering the compromised devices useless. Recordings cannot be made on these devices, and recordings made by compliant devices using new media will not play on compromised devices.

Older, compliant devices can still use blank media containing updated DKBs.

---

[4] As one might image, the DKB can be quite large, but clever mathematics and a tree topology allow it to remain a manageable size.

[5] Distinct versions or applications of computer software contain different sets of Node Keys.

Older media containing out-of-date DKBs will still be useable by both old and new devices.

Thus, the Vidi system ensures that ordinary compliant users are not inconvenienced by the malfeasance of those few who attack the system.

Software applications of a particular version all have the same Node Key set and are excluded by version, but software is readily upgraded. Hardware devices each contain a distinct Node Key set and are excluded on an individual basis. Hardware compromises of any significance are expected to be relatively rare. Thus, Vidi accommodates the most likely types of compromise with minimal effect on ordinary compliant users.

3.2.2 Renewability/Device Revocation

In the event that an individual, using extraordinary measures, is able to compromise (i.e., extract keys from) a Vidi-compliant device (either a hardware or software implementation) such that it results in a widespread deployment of compromised keys (such as would occur with their publication on the Internet), the Vidi system is armed to repel such an attack by renewing its protection and making the device useless for the purpose of interacting with any new Vidi media going forward.

Each Vidi device contains a set of keys that permit access to one of the keys in the DKB written on the Vidi DVD. One of the keys in a compliant device will be able to access the so-called Root Key KR, which allows playback or recording of encrypted content on that specific Vidi DVD. In the event a Vidi device or Vidi software is attacked, future blank Vidi DVDs will no longer contain a version of the Root Key which is accessible to the compromised device key set.[6]

In this manner, the DKB functions much like a guest list: it enumerates which devices or software are permitted to participate in the system. Initially, all Vidi-compliant devices in the network will participate in the system. However, if some devices (inevitably) become compromised, the Vidi system uses a carefully-crafted procedure (designed especially to prevent wrongful revocation) whereby those devices will be identified by the operators of the Vidi system, who will then update the DKBs of all future blank Vidi DVDs such that they will not authorize the compromised devices. Compromised devices rapidly become useless with release of new blank media.

---

[6] The Vidi system employs two authentication systems. The first is the Disc Key Block DKB, which is contained on all blank Vidi DVDs, and which is used to authorize Vidi devices and Vidi software applications. The second is the Application Key Block AKB, which is contained in all Vidi software applications and used to authorize compliant Vidi computer drives (see discussion in Section 4.10). In both systems, the structure of the key blocks and the method of revocation are the same.

3.2.3 Interoperability

The Vidi system will completely and seamlessly interoperate with any and all other digital broadcast content protection and recording technologies approved for use with the Broadcast Flag by the FCC.[7] Because the Vidi system focuses exclusively on only one "link" in the "chain of custody" required to protect content in an encryption environment – protection of content when stored on removable media – full interoperability with all other technologies handling that content not only is desirable, it is essential.

3.2.4 Scope of Redistribution

The goal of protecting digital broadcast content from unauthorized redistribution is by definition somewhat limited. Under the current system, digital broadcast content is widely distributed over the air to large numbers of households at a time of the broadcasters choosing. By broadcasting content in this manner, we acknowledge that content, and indeed copies of this content will appear in many households in the reception area. What the regulation seeks to avoid is a "secondary" redistribution on a wide scale to regions outside the original broadcast region or even within the broadcast region at a time different from that of the original broadcast.

As discussed, the Vidi system is part of a complex encryption system designed to maintain a "chain of custody" for content marked with the broadcast flag. From the moment content is received from an off-air antenna or a cable system, the content is protected from indiscriminate redistribution over the Internet. The scope of protection afforded by Vidi focuses exclusively on one component in this chain of custody: it protects content that has been stored on removable media, and prevents the movement of protected content to non-compliant devices. Thus, the Vidi system prevents indiscriminant redistribution as follows:

- Removable media containing Vidi protected content can only be played by compliant devices (including PC DVD drives), none of which will redistribute content indiscriminately; and
- A compliant device will only output digital forms of the protected content played from a Vidi disc using approved output technologies, none of which will redistribute content indiscriminately.

Therefore, the Vidi system contributes to this "chain of custody" by preventing content from appearing in digital form that is usable by devices that will permit indiscriminate redistribution of digital broadcast content.

---

[7] As discussed in Section 5.1 below, the Vidi license envisions and welcomes such interoperability, and does not require the use of any particular link protection system in Vidi-compliant devices. The Vidi license requires a Vidi device to accept the marking signals from the ATSC RC Descriptor or from an FCC-approved "Authorized Output Protection Technology" or "Authorized Recording Method."

4 Detailed Analysis of The Level of Protection Afforded By Vidi

4.1 Resistance to Known Threats

In order to demonstrate the capabilities and robustness of the Vidi copy protection system, the most common types of attacks are outlined here along with a description of how the Vidi system is resistant to these threats. This list of threats is not intended to be exhaustive. The Vidi system is, in practice, resistant to many more attacks than those outlined below.[8] This list merely represents the most common threats faced by content protection systems of this type.

4.1.1 Bit-for-Bit Disc Copy

Description of Attack: An attacker attempts to make an unauthorized copy of a Vidi protected disc by making an exact copy of all or a subset of the protected video content on the Vidi disc.

Protection Mechanism: This type of attack is not useful because each Vidi DVD contains a Unique ID which is used in the protection of the content and is required to play the recorded, protected content. This unique piece of information is stored in a location on the disc that is blocked by the device from recording user data. Since this unique piece of information cannot be copied, a bit-for-bit copy is useless to an attacker since it cannot be properly decrypted and played.

4.1.2 Emulation of Vidi-capable Computer Drive

Description of Attack: An attacker misuses a DVD-recordable computer drive, or hard disc drive, to emulate the functionality of a Vidi-capable device. Such an emulated drive would attempt to trick a compliant Vidi-capable software application into making recordings that the emulated drive will expose in non-protected, form.

Protection Mechanism: Vidi-capable software applications will only operate with a computer drive that can be authenticated (see Section 4.10) as a valid, Vidi-capable computer drive.

4.1.3 System Secrets Revealed

Description of Attack: One or more of the system secrets (such as the Node key set) of a Vidi-capable player/recorder or software become compromised and disclosed to the public.

Protection Mechanism: The Vidi robustness and compliance rules specify a secure manner in which system secrets should be maintained and protected. If followed carefully, this should ensure that the extraction of system secrets remains difficult.

---

[8] A copy of the Vidi specification, "Vidi Copy Protection System for DVD+R/+RW Video Recording Format – System Description," Version 1.0 (March 1, 2004) is attached at Appendix A.

However, if a successful attack is made on a particular device or software version, the secret values used by Vidi are fully revocable and renewable as future blank Vidi media will contain DKB's excluding the compromised Node Key set thus limiting the damage this revelation can cause. Similarly, software which contains an Application Key Block AKB will not be able to authenticate a revoked drive and will refuse to pass certain critical information between the PC software and the revoked PC drive.

4.1.4 Cryptographic Attack

Description of Attack: A person or large team of attackers attempts to exploit weaknesses in the chosen cryptographic algorithms used by Vidi or, through the marshalling of a large number of machines, attempts to break the keys used by Vidi in a "brute force" attack.

Protection Mechanism: Vidi makes use of proven cryptographic algorithms and protocols. While there is no guarantee that someone will not discover a weakness in these algorithms, they have been used for many years and subject to open review by the cryptographic community and have to date not been compromised. This method (placing an algorithm in the public domain and allowing anyone who wishes to probe for weaknesses) is the gold standard for testing cryptographic algorithms.

As for a brute force attack, the key length used by the cryptographic algorithms is 128 bits. Even if an attacker could harness the processing power of all of the existing machines in the world today, it would take hundreds of millions of years (conservatively) to crack a single 128-bit key. In any case, such an attack would likely compromise only a single Vidi recording.

4.1.5 Software Player Compromise

Description of Attack: A Vidi-capable software player is disassembled by a hacker and modified to allow unauthorized copying of video content, or a hacker distributes a software tool that perverts a compliant Vidi-capable software player into exposing protected content.

Protection Mechanism: The revocation criteria associated with Vidi allow for the revocation of the Node Key set use by the compromised software application. Future blank Vidi media will contain DKBs excluding the compromised Node Key set thus limiting the damage this revelation can cause.

4.1.6 Hardware Tampering

Description of Attack: An attacker attempts to modify a Vidi-compliant DVD+R/+RW drive to circumvent the security features through manipulating switches on the motherboard or disabling specific semiconductor chips.

Protection Mechanism: The robustness rules associated with the Vidi copy protection system do not allow manufacturers to have switches present on the motherboard that can disable the copy protection mechanisms. Furthermore, products shall be designed and implemented such that the content protection system, as specified by the Specifications and Compliance Rules, cannot be defeated or circumvented merely by an ordinary user using generally available tools or equipment.

4.1.7 DKB Modification

Description of Attack: A malicious user replaces the pre-recorded DKB on a blank disc with an old (compromised) DKB.

Protection Mechanism: Recorders are required to check whether the hash of the DKB matches the copy of the DKB written in the ADIP.[9] That copy cannot be changed because data in the ADIP cannot be modified. Recorders will therefore detect tampering with the DKB, and refuse to record on a disc modified in this manner.

4.1.8 CCI Bit Modification

Description of Attack: A malicious user modifies the Copy Control Information ("CCI") bits associated with protected content and changes the bits from the Copy One Generation (COG) state to the Redistribution Control (RC) state to allow unlimited copies.[10]

Protection Mechanism: The Vidi copy protection system protects the original CCI state associated with the content by storing it in a special, protected manner in the CCI-MAC (Message Authentication Code). Vidi-compliant players are required to check the CCI-MAC and, if the CCI state does not match the CCI-MAC state, to use the more restrictive of the two states. This effectively prevents the modification of the CCI state. Modification of the CCI-MAC would require a compromise of the AES algorithm or revelation of keys. Both of these types of attacks have been described earlier.

4.2 Cryptographic Functions

Since the chosen system for protection is an encryption system, we must specify fundamental encryption algorithms to accomplish two tasks:

Encryption – This is the process of concealing digital data by means of an algorithm using a key. If one has the key, decryption is easy. Reading the data without the key should be insurmountably difficult.

Hashing – A "mixing" or binding process, hashing combines two or more pieces of data resulting in a small "fingerprint" or representation of data. Hashes are used to create dependencies on precise correctness of data. On average, half of the bits of the hash (also known as the "fingerprint") will change if even one bit of the data changes. This is true even if data being hashed is very large.

4.2.1 Encryption Algorithm

The encryption algorithm used by Vidi is the Advanced Encryption Standard (AES). AES is a block cipher, which encrypts 128 bits (the block size) at a time using, in the case of Vidi, a key size of 128 bits. AES was adopted by NIST as US FIPS PUB 197 in November 2001 and is used by financial institutions, the U.S. government and other areas

---

[9] The ADIP is a special, pre-pressed spiral track on a Vidi DVD. See also Section 4.3.

[10] While not strictly relevant to the Broadcast Flag, this scenario underscores Vidi's ability to do no harm to other existing content protection systems.

where proven security is required. The 128-bit key size makes it essentially impossible to search through all of the keys using computers.

AES also can operate in several different modes of operation used to encrypt multiple blocks of data. Vidi has chosen to use AES in Cipher Block Chaining (CBC) mode, a mode that binds a group of 128-bit blocks into a single encrypted block.

4.2.2 Hash Algorithm

The hash algorithm chosen for use by Vidi is based on AES as its principal security element. The Vidi hash algorithm divides the data to be hashed into 128-bit blocks and applies the hash algorithm serially to the blocks of information. If the data does not divide evenly into 128-bit blocks, the final block is completed using zeroes. The resulting fingerprint is 128 bits long and can be used as key for encryption operations.

4.2.3 Random Number Generator

Vidi depends on the generation of cryptographically secure random numbers. To be secure, random numbers can in no way be predictable. There are 2 types of random number generators: true random number generators (which rely on some random source in nature to create random numbers) and pseudo-random number generators (which generate a sequence of numbers, the elements of which are approximately independent). Vidi requires the use for either a true random number generator or a pseudo-random number generator that passes a set of specific tests of randomness. The test set is defined in NIST standard FIPS 140-1.

4.3 The DVD+RW Optical Disc Format

Just like an old fashioned vinyl 33 RPM recording, DVD+RW and DVD+R discs have a continuous spiral “track” where data is kept, and just like any such recording there is a “lead in” area where the beginning of the recorded data starts. This spiral track (or groove) contains addressing information called Address In Pre-Groove (ADIP) to determine where to write on the disc. The ADIP is distributed across the entire disc and also contains extra information beyond the addressing information. The ADIP area is stamped into every DVD+RW disc by a "master” disc as part of the manufacturing process. Information stored in the ADIP cannot be modified by recording equipment, even though the disc is a recordable DVD. Information in the ADIP can only be read. Vidi DVDs contain additional information in the ADIP, such as the DKB and the cryptographic hash (or fingerprint) of the DKB. By storing the DKB and DKB-hash in the read-only ADIP, Vidi prevents DKB modification by hackers.

4.4 States of the Vidi DVD

4.4.1 Blank State of a Vidi DVD

Each new, blank Vidi DVD contains the DKB in the ADIP area of the disc. As discussed above, the DKB essentially is an authorization list of properly licensed Vidi devices. If a particular Vidi device is compromised (for instance, if its secret Node Keys are published on the Internet), future versions of Vidi media will not contain the authorization for these

compromised devices. Thus, the system is continually renewed (as explained in Section 3.2.2), to prevent the widespread misuse of the Vidi system.

4.4.2 Clear State of a Vidi DVD

If a protected recording is never made on a Vidi disc, the media behaves like an ordinary DVD+RW disc and recorded data is not encrypted.

4.4.3 Protected State of a Vidi DVD

When the first protected recording is made on a Vidi DVD, a random key KU is created immediately and used to create a protected recording. At a later time, the KU is encrypted by a key called KD and stored on the disc. At the same time, the DKB is copied from the ADIP and stored twice in Buffer Zone 2 for performance reasons. Likewise, a unique ID is created by the drive and placed in the header of every sector in Buffer Zone 2 that contains the DKB. The repetition of the DKB and Unique ID improves performance of the hardware and resists damage to the disc.

4.5 Disc Keys and Data Layout

In addition to the DKB, and the Root Key stored in the DKB, the Vidi system makes use of several different types of keys for various security purposes. These include the:

- Unique ID, a random unique identification number that is created and written onto the disc when the disc is first inserted in a Vidi recorder;
- Disc Key KD, created when the Root Key KR is “hashed” together with the Unique ID;
- Unique Key KU, created by means of a secure random number generator when the first protected recording is made on a Vidi DVD;
- Program Key KP, created via a secure random number generator and encrypted with the Unique Key KU;
- Sector Key KS, created by hashing the Program Key KP with part of the video content being protected.

4.5.1 Unique ID

Every Vidi DVD shipped is blank except for the DKB in the ADIP area. When the disc is first inserted in a Vidi recorder, a random unique identification number (Unique ID) is created and written onto the disc in Buffer Zone 2. The Unique ID is always used as a contribution for all encryption of keys or content on the Vidi disc, thereby binding the content to this particular disc. Thus, an attack compromising content on one Vidi DVD will not provide any assistance in compromising content on a second (or any other) Vidi DVD. Transfer of encrypted content from one Vidi DVD to another can be accomplished only with Vidi-enabled devices that abide by the CCI rules that are initially recorded with the content (see discussion in Section 4.5.5).

4.5.2 Disc Key KD

Hashing the Root Key KR together with the Unique ID creates the Disc Key KD. KD represents both the uniqueness of this particular disc and the acceptance of the recorder as a compliant component of the Vidi security system. KD is not stored but is created, used and discarded as part of the normal operation of the Vidi system.

4.5.3 Unique Key KU

When the first protected recording is made on a Vidi DVD, a Unique Key KU is created by means of a secure random number generator. This key is encrypted with KD and stored in the file "Video_RM.IFO." This file exists on every DVD+RW disc containing DVD formatted video; however the encrypted KU is stored only if the Vidi disc is used for protected video. There is only one such file on the Vidi DVD. If a previously protected recording has been made on a particular Vidi DVD, the KU can be reused for other protected recordings. Copying the file Video_RM.IFO will not enable access to protected recordings because the Unique ID on the second Vidi DVD will not match the Unique ID of the disc from which the file was copied.

4.5.4 Program Key KP

Program keys are created when: (a) a new protected video recording is being made; (b) when the CCI status of the incoming video changes; or (c) if the recorder decides it is necessary (but never more frequently than every 10 seconds of video). The program keys are changed frequently to ensure that the recorder is not deceived into recording protected video in an incorrect state, *i.e.,* recording Copy One Generation (COG) content in the (more freely copy-able) Broadcast flag state. The Program Key KP is created via a secure random number generator and is encrypted with the Unique Key KU. Program Key KP is placed in navigation packs associated with protected video.

4.5.5 Copy Control Information

Copy Control Information comes in five states: Copy Never, Copy One Generation, Copy Freely, Copy No More and Copy Freely but do not Redistribute Indiscriminately (called the Redistribution Controlled, or "RC," state – *i.e.*, digital broadcast content). A Vidi recorder will refuse to copy the Copy Never or Copy No More content and no security is required for Copy Freely content. Therefore, all stored content protected by Vidi will be in the Copy No More or RC state.

In addition to the Program Key KP, the navigation packs for protected video also contain a CCI-MAC designating restrictions on the use of the protected video. The CCI-MAC is encrypted with KP to ensure that CCI cannot be changed from COG to RC, and includes several copies of the CGMS control bits that define the above states together with some APS trigger bits (to trigger an analog protection system such as Macrovision). All of these are hashed and the encrypted with KP.

4.5.6 Protected Video

Video is divided into 2048-byte sections matching the data sectors on the disc. The first 128 bytes of video are always left in the clear so that navigation (FF, Rewind, etc.) can be activated immediately, without waiting for decryption of the initial bytes. The remaining

1920 bytes are encrypted via AES Cipher Block Chaining (AES-CBC) using a Sector Key KS.

4.5.7 Sector Key KS

The Sector Key KS is created by hashing the Program Key KP with part of the video content being protected. Thus, every sector has its own key, which hides the program key from an attacker. The encryption of each sector depends on the Program Key KP, which is further dependant on the DKB and Unique ID, as well as the content itself. Sector Key KS is not stored, but rather is re-created and used whenever it is needed.

4.6 Recording and Playing Content

The Vidi security system has only two functions: the recording of protected content and the playback of protected content. Each of these functions depends on secure communication between a Vidi DVD and the recorder or player. In some cases, the communication path will be secured physically (*e.g.,* in a consumer electronics device). However, in the case of a software player, an authentication protocol will be implemented in order to secure the communication between the software player and the Vidi drive.

4.7 Initialization of a Blank Vidi Disc

When a Vidi disc is created, it contains a system of navigation cues particular to the DVD+RW format. These navigation cues allow a Vidi recorder to locate the DKB stamped in the ADIP portion of the disc. When the first secure recording is made by the Vidi system the DKB is copied from the ADIP area to the Buffer Zone 2 area. At the same time, a Unique ID is created and written into the Buffer Zone 2 area. Secure recordings are only completed and readable if the DKB has been copied and the Unique ID has been written. In the case of the first protected recording, storage of the Unique ID and DKB is done in parallel with recording of the content, as described in step 3-A below. This optimization improves user performance for the first protected recording on a Vidi DVD. Subsequent protected recordings will follow the numbered steps outlined below, using step 3-B instead of step 3-A.

4.8 Secure Recording Process

Assuming that the disc has been initialized, when a secure recording is being created, one must encrypt the video as it is recorded. Encryption requires a series of keys, each of which must be dependant on several elements, including the DKB, the Unique ID and the data itself. By creating keys in this manner, we ensure that attacking one key in the Vidi system will only bring a small portion of a single video recording into the clear. Likewise, we prevent the improper transfer of data from one Vidi disc to another. Only compliant devices can make playable recordings thus preventing ordinary users from copying encrypted files from a Vidi disc to a hard drive or another Vidi disc via the Internet.

4.8.1 Steps in the Secure Recording Process

Step 1-A – If this is the first protected recording on this disc, the DKB is retrieved by the drive from the ADIP and copied to the Buffer Zone 2. In addition, the Unique ID is generated by the drive and stored along with the DKB in the Buffer Zone 2. The Root Key KR is then derived from the DKB using the Node Keys KN and the Device ID.

Step 1-B – If the DKB has already been copied to the Buffer Zone 2, the DKB is retrieved by the drive from Buffer Zone 2 on the disc for processing. The Root Key KR is then derived from the DKB using the Node Keys KN and the Device ID.

Step 2 – The intermediate Disc Key KD is created by hashing the Root Key KR with the Unique ID. The Unique ID is stored in Buffer Zone 2 along with the DKB. Thus, all content encryption keys are bound to this particular disc and, even if compromised, cannot be used to decrypt any other disc. Disc Key KD is not kept by the drive nor stored on the disc.

Step 3-A – If this is the first protected recording on this disc, a random key is created by the drive and designated the Unique Key KU. The Unique Key KU is then encrypted with Disc Key KD and stored on the disc in the file Video_RM.IFO. A copy of Unique Key KU is kept for use in step 4.

Step 3-B – If an encrypted Unique Key KU already exists on the disc, it is retrieved from the disc and decrypted by Disc Key KD.

Step 4 – For each new protected recording, a random Program Key KP is created by the drive. A new Program Key KP will also be created each time the CCI of the input video changes and when the recorder deems it necessary but not more often than every 10 seconds of video recorded. Each Program Key KP is encrypted by Unique Key KU and stored on the disc in the appropriate navigation pack. The CCI is embedded in a CCI-MAC[11] and encrypted with Program Key KP.[12]

Step 5 – For each 2048-byte segment of video, a new intermediate Sector Key KS is created. The Sector Key KS is formed by hashing bytes 80-95 of each video sector together with the Program Key KP.

Step 6 – The first 128 bytes of each sector are not encrypted in order to allow for rapid user navigation of content. The remaining data is encrypted with Sector Key KS and stored in the same manner as unencrypted video. After Sector Key KS is used to encrypt a sector, it is discarded. Sector Key KS will be recreated when needed for playback.

4.9 Secure Playback Process

With the Vidi system, only Vidi-compliant devices, including PC-based DVD players, are permitted to play protected recordings, thus preventing ordinary users from viewing

---

[11] "Vidi Copy Protection System for the DVD+R/+RW Video Recording Format – System Description," Version 1.0 (March 1, 2004) at Section 6.4.1.

[12] In contexts other than the Broadcast Flag, encrypting the CCI prevents conversion of Copy One Generation content to Redistribution Content.

encrypted files from a Vidi DVD on a non-compliant device. To accomplish this, the DVD player extracts the Root Key KR from the DKB and uses this key to calculate the key used to protect the content, after which the protected content is decrypted and displayed.

4.9.1 Steps in the Secure Playback Process

The specific steps of the secure playback process are as follows:

Step 1 – The DKB is retrieved by the drive from the disc for processing. The DKB is needed to compute the disc Root Key KR. Only compliant devices can compute Root Key KR from the DKB using the Node Keys KN and the Device ID.

Step 2 – The Unique ID is retrieved from the disc and hashed with Root Key KR to form the Disc Key KD.

Step 3 – The encrypted Unique Key KU is retrieved from the disc and is decrypted using Disc Key KD.

Step 4 – The encrypted Program Key KP for the program to be played is retrieved from the appropriate navigation pack and is decrypted using Unique Key KU.

Step 5 – The Sector Key KS is formed by hashing bytes 80-95 of the sector (which are always in the clear) together with the Program Key KP.

Step 6 – The first 128 bytes of each segment are played directly (these bytes are always in the clear). The remaining data is decrypted with Sector Key KS and played just as would be unencrypted video.

4.10 Authentication Protocol in a Computer Environment

Recording and playing involves the use of security elements, *i.e*., keys that cannot be revealed. In a CE device, the communication is protected by the physical environment: the keys are moved inside hardware and cannot be easily acquired by an outside party. However, where a DVD recording is made in a PC environment – which is specifically designed to enable users to gain access to its systems, and where keys must pass through numerous cables and software elements (*e.g.,* an operating system and drivers) – additional steps are required to guarantee the PC application and the Vidi-enabled DVD+R/+RW drive can communicate in a secure manner.

No method exists currently to prevent the "tapping" of, or "listening-in" on, communication between a hardware device, such as a Vidi drive, and a software player/recorder. Therefore, a secure authentication protocol must be used when communicating between the Vidi drive and a software player/recorder.

Typically, computer systems place most of the intelligence in software applications rather than hardware. Therefore, it is expected that the software application will contain the key node sets required to operate with a Vidi disc, and that the hardware drive will act as a simple pass-through device. However, the software must determine if the hardware device with which it is communicating is a valid, compliant device or a simply a sophisticated software simulation of a valid device. Vidi therefore establishes the following authentication protocol between a compliant Vidi application and a compliant

Vidi hardware drive to ascertain that the hardware drive is compliant and to ensure that communication between the software application and the compliant drive is not intercepted and misused by malicious software.

Thus, the purpose of software-hardware device authentication is twofold:

1. To ensure that the application software is conversing with a compliant hardware drive and not a nefarious software application mimicking a Vidi computer drive; and
2. To ensure that elements used to create keys such as the Unique ID from the Vidi disc is not intercepted by an attacker

Following authentication of the PC drive by the application software, either the playback (described in Section 4.9) or recording process (described in Section 4.8) must be followed (see Figure 1).

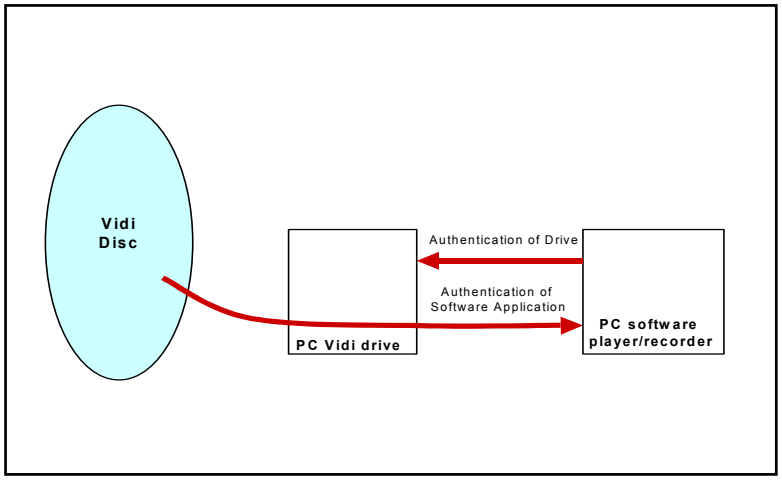

Figure 1

4.10.1 Initial Conditions

Each Vidi PC drive contains a unique Device ID_d and a set of device node keys KN_d. The Vidi software application will have a special authorization DKB called an Application Key Block AKB and an authentication Root Key KR_{auth}. It should be clear that the Application Key Block AKB system used to authenticate a Vidi drive to Vidi software applications has no connection to the DKB system used to authorize Vidi devices and software applications to Vidi discs.

4.10.2 Steps in the Authentication Process

Step 1 – The software application sends a request to the drive for the Device ID_d.

The drive sends the Device ID_d to the software application.

Step 2 – The software application uses the Device ID_d to find the appropriate Authorization Key KA_x inside the Application Key Block AKB. The software application saves the variable j which represents the number of the node key that the drive should use.

The software application creates a random number RA using a secure random number generator and sends the collection of j || RA || KA_x to the drive.[13]

Step 3 – The drive uses its j'th Node Key KN_j to encrypt KA_x yielding KR_{auth}. The computed KR_{auth} is the same key that is held by the software application.

Step 4 – The drive creates a random number RD and a key contribution QD and sends the following message RA || RD || QD encrypted with the key KR_{auth} using licensed constant IV2.

Step 5 – The software application decrypts the message using KR_{auth} and verifies that RA is identical to a saved version of RA. Verifying that the RA that comes back is identical to the sent RA proves that this communication is new and not a copy of a previous communication with compliant Vidi device.

Step 6 – The software application creates a key contribution QA and decrypts the following message RD || RA || QA with KR_{auth} again using the licensed constant IV2. The software application then calculates the bus key KB by hashing QD || QA.

Step 7 – The drive encrypts the message using KR_{auth} and verifies that RD is identical to a saved version of RD. The drive then calculates the bus key KB by hashing QD || QA. Verifying that the RD that comes back is identical to the sent RD proves to the drive that the communication is new and a copy of a previous communication with compliant Vidi software.[14]

Step 8 – The software application requests the DKB Hash and Unique ID from the Vidi disc.

If the drive is playback-only, the DKB Hash is set to all zeroes. In any case, the drive encrypts the message DKB Hash || Reserved || Unique ID with bus key KB again using the licensed constant IV2 and sends it to the software application, where the normal Vidi key processing begins for playback or recording.

Recording or playback can now begin.

---

[13] The || symbol implies concatenate or append.

[14] Computation of the Bus Key KB using contributions from both the drive and the software ensures that a new key is created for each communication session limiting an attack on that key to compromising only a single device.

5 Vidi Will Be Made Available on a Reasonable and Nondiscriminatory Basis on Terms that Protect Competition and Innovation

5.1 Overview

As evidenced by the "Vidi Content Protection Agreement" (attached hereto as Appendix B), Vidi will be made available on reasonable and nondiscriminatory terms and conditions. The technology agreement will be made available under a standard form agreement to any interested implementer or content participant. In order to promote transparency, a single form agreement is used for all implementers and content participants, regardless of the rights they seek. The agreement itself contains a covenant (§13.9) obligating Philips and HP to make rights to use Vidi available on "fair, non-discriminatory and equal terms," and granting parties the right to obtain the same terms given to any other party if the terms should change. The fees included in the form agreement are generally below those charged for other content protection systems.

The agreement contains numerous safeguards to protect competition and ensure that implementers and content participants alike will be treated fairly. Content participants are granted third party beneficiary rights to restrain material breaches of the agreement that are likely to compromise security. The agreement avoids first-mover advantage by permitting only very limited changes to the Specification and associated Compliance and Robustness Rules, and by requiring an open process that includes both content participants and implementers before any change becomes effective. Implementers are not required to sign away their own intellectual property without compensation under a reciprocal non-assert. They are simply required to agree to license necessary patent claims in a reasonable and non-discriminatory manner, under an obligation similar to that contained in the DFAST license agreement.

The compliance rules applicable to Unencrypted Digital Terrestrial Broadcast Content are modeled after the rules applicable to Covered Demodulator Products directly subject to the FCC's own regulation. This ensures a consistent level of content protection throughout the system and further protects implementers from the risk of overreaching changes to the rules by Philips. Most notably, this means that a Vidi licensed player may output recorded broadcast flagged content over any digital output technology approved by the FCC for use by a Covered Demodulator. Thus, Vidi cannot serve as a bottleneck against other technologies.

The Robustness Rules clearly meet the ordinary user standard established by the Commission. They are more detailed than the rule set forth in § 73.9007 to account for the fact that the technology is also intended to be used for content subject to copy control (e.g., Copy One Generation content) received from devices under the DFAST license.

5.2 Business Terms

To maximize transparency, Vidi will be offered under a single agreement for all implementers and content participants. The agreement specifies which provisions apply to each of the different classes of implementer and content participants. The different classes of implementers correspond to the different roles implementer may wish to fill. These include: hardware and software recorder/player manufacturers; component manufacturers (e.g., chip manufacturers); disc master manufacturers; and blank disc replicators. Each is granted the rights necessary to perform their relevant function. Fees and reporting obligations vary with the functions. Obligations are imposed only to the extent considered necessary to preserve the security of the system.

5.2.1 Rights Conferred

Philips and HP agree, with respect to the activities relevant to each implementer role, not to assert the intellectual property they each have in Vidi against the use of Vidi within the relevant "Field of Use," defined as the use of Vidi to encrypt audiovisual content on DVD+R and DVD+RW discs, the use of Vidi to decrypt such content for playback from such discs, and the embedding of keys in blank discs. Agreement §§ 1.2, 2.1. In each case, the agreement not to assert IP extends to making, using, and selling, among other rights. Philips and HP further agree not to assert their IP rights in Vidi against Content Participants for causing the use of Vidi to protect audiovisual content within the Field of Use. Agreement § 2.1.6. All of the agreements not to assert IP are subject to conformance with the Specification and the Compliance Rules. In addition, a limited covenant not to assert IP is granted in favor of those who wish to use Vidi solely for the development of products and components. Agreement § 2.2.

There is no limitation on the sale of finished, compliant, hardware and software products. Components that are not complete products but that contain secret device keys may only be sold to authorized product manufacturers. Agreement § 2.3.3. Components such as chip sets that do not contain device keys may be sold to anyone. Masters and stampers (sub-masters) used to create blank discs that contain keys may only be sold to authorized blank disc replicators. Agreement §§ 2.3.1, 2.3.2.

5.2.2 Reciprocal Licensing Covenant

Implementers and content participants alike are required to agree to license any patent claims necessary for the use of Vidi on reasonable and nondiscriminatory terms. Agreement § 2.5. This requirement parallels the requirement of the DFAST license (§ 3.5). Thus, implementers are not required to sign away their own intellectual property without compensation under a reciprocal non-assert. As a result, the agreement does not discriminate against IP owners who also happen to be implementers or charge more to implements who also happen to be IP owners by requiring them to forfeit their intellectual property without fair compensation.

5.2.3 Fees

Vidi fees are lower than those charged by most other content protection technologies. Implementers are not subject to an annual fee. There is a one-time € 5,000 fee upon execution of the agreement. The one-time fee is not cumulative, such that any

implementer that engages in multiple areas requiring a license is limited to just the € 5,000 fee. Agreement § 3.1a. Component implementers do not pay any additional fee. A per device key fee of € 0.05 (five Euro cents) is charged for each device key used by a hardware manufacturer. Agreement § 3.3.1. In addition, there is an administrative fee of € 220 for each disc containing up to 32,768 device keys. Agreement Ex. B. Replicators must pay a per disc fee of € 0.01 (one Euro cent). Agreement § 3.3.5.

Software manufacturers and disc master manufacturers are not subject to any key fee. Software manufacturers pay only an administrative fee of € 750 for a disc containing software keys and Application Key Blocks. Disc master manufacturers pay only an administrative fee of € 750 for a disc containing software keys and Disc Key Blocks.

Content participants, who are not subject to key fees, are subject to an annual € 10,000 fee. Agreement § 3.1b.

Key fees are not subject to change. Administrative fees are subject to change only to reflect the actual cost of administration. Agreement § 3.2.

5.2.4 Reporting and Confidentiality of Implementer Information

Replicators are required to submit quarterly reports and payments setting forth the number of blank discs sold or otherwise disposed of. Agreement Art. 4. Hardware implementers and master manufacturers are required to keep records showing the number of keys ordered and demonstrating to whom components containing device keys and masters and stampers, respectively, were distributed. An independent accountant may audit those records. Agreement Art. 5. The content of replicator reports, reports from any audits, and information concerning the number of keys ordered are considered confidential information and will be protected by Philips and walled off from any employees responsible for the manufacture or sale of Vidi products or products that compete with Vidi products. Agreement § 8.2.

5.2.5 Vidi Confidential Information

Vidi will impose minimal confidentiality obligations on users. The only information treated as confidential will be the Licensed Constants (which are provided to hardware, software and component implementers) and the device keys, which are treated as "highly confidential information." Agreement §§ 8.1, 8.3. Device keys are provided only to hardware and software implementers.

5.2.6 Changes in Specification and Compliance Rules

The agreement permits only very limited changes to the Specification and associated Compliance and Robustness Rules and requires an open process that includes both content participants and implementers before any permitted change becomes effective. In this way, implementers are protected from any first mover advantage that could otherwise result in favor of Philips and HP. Further, the technology is defined and set, and may be relied upon to produce products. The following types of changes are permitted: (i) fixes to correct errors, omissions or bugs, subject to certain limitations; (ii) changes to add analog outputs, as long as they are no less protected than analog outputs approved under

DFAST, CSS, Vidi, or any rule that may in the future be adopted for analog outputs by the Commission; (iii) changes to conform to a government mandate. Agreement § 6.2.

The agreement obligates Philips to notify implementers and content participants as soon as a change is under serious consideration and provides an opportunity for implementers and content participants to comment on the proposed change. The agreement provides for consultation to reconcile objections to the proposed change. Agreement §§ 6.3.1 to 6.3.4. If objections cannot be reconciled, objecting parties may invoke arbitration to prevent the change. Agreement § 6.5.

The agreement does not preclude Philips from expanding the functionality of Vidi or extending it to other video or media formats. However, such extensions will be offered under separate agreements or addenda and will not be mandatory.

5.2.7 Revocation of Devices

Article 7 and Exhibit D of the agreement covers device revocation. Keys may be revoked in limited circumstances in order to protect users against loss of functionality. A hardware device key may be revoked only if the same hardware key is found in more than one device or product, the implementer has disclosed the key, or the key has been lost, stolen, or otherwise misdirected. A software key may be revoked only if the key is found in applications widely used in conjunction with unauthorized copying or distribution, the key has been lost stolen or otherwise misdirected or is made public, or if the software key is used in a hardware device. Exhibit D establishes a procedure, including arbitration, to protect against inappropriate revocation. Device revocation also is discussed above at 3.2.2.

5.2.8 Remedies

The agreement defines material breach, and provides for injunctive relief against such breaches. Substantial, but fair, liquidated damages are provided for those types of material breaches most likely to compromise the security of Vidi or content protected by Vidi. Content participants are granted third party beneficiary rights to seek injunctive relief if they are a producer of audiovisual content with annual turnover of more than € 100,000,000 from production, transmission or distribution of such content and are in compliance with their obligations under the agreement.

5.2.9 Term and Termination

The term of the agreement runs through July 1, 2014, subject to renewal for successive terms of 5 years unless either party notifies the other that it does not wish to renew. Implementers and content participants have the right to terminate at any time on 90 days' notice. There is provision for termination for uncured material breach, if the breach is either the result of non-payment, conduct that would give rise to liquidated damages, or failure to use reasonable measures to prevent frequent device key revocation, if device keys have been frequently revoked.

5.3 Compliance and Robustness Rules

5.3.1 Compliance Rules

The compliance rules applicable to content that is subject to redistribution control but not copy limitation (i.e., Unencrypted Digital Terrestrial Broadcast Content as defined in the broadcast flag rule, or EPN content as defined by some other content protection systems) are modeled after the rules applicable to Covered Demodulator Products directly subject to the FCC's own regulation. The goal is to ensure a consistent level of content protection throughout the system without imposing restrictions downstream that limit manufacturers and consumers but provide no security benefits. The Vidi approach further limits the risk of overreaching changes or obligations beyond those directly deemed appropriate by the Commission.

Just as the Commission's broadcast flag rule currently imposes no limitations on analog outputs for broadcast flag content, the Vidi rules impose no such limitations on analog outputs for broadcast flag or EPN content. See Ex. A § A.1.2.1.

Any digital output approved by the FCC for use by Covered Demodulator Products is automatically deemed approved for use by a Vidi player to output EPN content. Ex. A § A.1.2.2.1 (referencing § 73.9004(a)). Similarly, the audio portion of EPN content may be output to any output permitted under the broadcast flag regulation, § 73.9005. Ex. A. § A.1.2.2.1. Analogously, although it is not relevant here, any content bearing the CCI state Copy No More may be output over any digital output approved under the DFAST license.

The Compliance Rules further obligate Vidi players to detect tampering by comparing copy control information in two different locations. Ex. A § A.1.2.4. Integrated products with a second recording function are permitted, but are limited to making those copies that could be made if the second recording function were in a separate housing and were connected with a permitted output.

In addition, in keeping with the requirements of the DFAST license, the CSS license and the current DTCP license, the Vidi Compliance Rules prohibit tampering with certain identified watermarks.

5.3.2 Robustness Rules

The Robustness Rules clearly meet the ordinary user standard established by the Commission in § 73.9007. Greater detail is provided that is modeled after the robustness rules set forth in the DFAST license to account for the fact that the technology is also intended to be used for content subject to copy control (e.g., Copy One Generation content) received from devices under the DFAST license.

6 Approval and Licensing of Vidi by Content Owners, Broadcasters and Device Manufacturers

Vidi is a new content protection system. Philips and HP will defer introducing the technology in the market and signing up licensees until such time as the FCC issues its approval for Vidi for use with the Broadcast Flag. Upon FCC approval, Vidi will be offered to content owners, broadcasters, and all potential implementers on reasonable, non-discriminatory and equal terms.

That said, Philips and HP are pleased to note the endorsement of Vidi by a number of key industrial partners:

Ricoh Company, Ltd. has made a detailed study of Vidi and believes Vidi provides adequate protection. Ricoh fully endorses application of this technology. http://www.ricoh.co.jp

Yamaha Corporation has made a detailed study of Vidi and believes Vidi provides adequate protection. Yamaha fully endorses application of this technology. http://www.yamaha.co.jp/

Ahead Software AG is one of the top 2 developers of optical disc creation software. Ahead has participated in the development of Vidi prototypes and software. Ahead's strong support for Vidi is significant in that it signals that software critical to the deployment of Vidi-enabled devices will likely be readily available should Vidi become an FCC-approved Broadcast Flag technology. http://www.ahead.de/

7 Advantages of Vidi Recordable DVD Protection System

The Vidi system meets the goals set by the FCC's broadcast flag regulation, allowing unlimited protected copying of Unencrypted Digital Terrestrial Broadcast Content, but fitting within the "chain of custody" to prevent indiscriminate Internet redistribution. The system assures a consistent level of protection by requiring playback devices to adhere to essentially the same rules for handling protected broadcast DTV content as are imposed on Covered Demodulator Products that are themselves directly subject to FCC regulation. As discussed, the Vidi system focuses specifically on one link in the "chain of custody" needed for an encryption based system. Such a focus offers several advantages:

7.1 Content Protection Advantages

1. Content is encrypted by the state of the art AES cipher. By using one of the best available encryption algorithms, Vidi provides unprecedented protection for content.
2. Long key length of 128 bits provides protection against an attack by exhaustive searching. Even if every computer on the planet were harnessed towards the effort of searching for a single AES key it would take literally millions of years to find the key. Such a calculation takes into account "Moore's law" regarding the improvement in computation speed provided by semiconductor technology. Other similar systems with shorter key lengths are potentially vulnerable to attacks over the expected lifetime of the broadcast flag protection system.
3. Keys are bound to physical media thus preventing a common attack of copying the entire encrypted content of a DVD.
4. A comprehensive system of keys including frequent key changes provides security against a "lucky guess" that uncovers a single key. Importantly, revelation of a single key will in no way endanger the system as a whole.
5. A device-specific revocation system that ensures rejection of devices or software if compromised by skilled attackers. Although the FCC requires only that an ordinary user find difficulty in attacking the system, Vidi provides a system of revocation so that an attack by a skilled person, distributed widely to ordinary users, is always limited. This is the main threat to software based protection systems and Vidi has a mechanism for addressing this threat.
6. Vidi extends device revocation to software revocation. Due to commercial requirements, a single version of software will have identical keys, thus attacking a single instantiation of that software leads to the compromise of all software of this type. When Vidi revokes these keys, all instantiations of this software are revoked simultaneously and effectively.

7. Vidi does not rely on the preservation of global secrets. All keys and other cryptographic information can be revoked and renewed. The system can recover in a robust manner from a security breach.

7.2 Consumer Protection Advantages

1. Vidi provides a comprehensive licensing program that allows revocation only after it is assured that ordinary consumers will not suffer from revocation of hardware.
2. Media purchased by consumers before revocation took place will continue to work on all devices.
3. Recordings that were made before revocation took place will continue to play on all devices.
4. Even if the only media available is Vidi media, legacy DVD+RW players will be able use Vidi media, but without the benefit of access to protected content.

7.3 Competition and Licensing Advantages

1. Vidi is made available in a non-discriminatory manner on reasonable and non-discriminatory terms and conditions.
2. Vidi ensures and does not restrain competition in content protection technology. Any technology approved by the Commission as an Authorized Digital Output Protection Technology is automatically approved for use by a Vidi licensed playback device to transfer Redistribution Controlled Content. A similar rule applies to Copy One Generation Content.
3. Vidi grants Content Participants third party beneficiary rights to restrain violations of the license terms that affect security. It also includes stiff liquidated damages against material breaches that threaten security.
4. Vidi does not discriminate against IP owners that also manufacture products. The Vidi technology agreement does not include a confiscatory reciprocal free non-assert. It requires only that users agree to license their necessary patents on reasonable and non-discriminatory terms.
5. Vidi protects users against over-reaching changes and potential first-mover advantage by limiting changes allowed under the agreement, and including a change management process that protects both content participants and implementers.

Appendix A

Vidi Copy Protection System
for the DVD+R/+RW Video Recording Format
System Description
Version 1.0
March 1, 2004

Vidi

Copy Protection System for the DVD+R/+RW Video Recording Format

System Description

Version 1.0

1 March 2004

PHILIPS

hp invent

COPYRIGHT

DISCLAIMER

The information contained herein is believed to be accurate as of the date of publication; however, neither Royal Philips Electronics nor Hewlett-Packard will be liable for any damages, including indirect or consequential, from use of the System Description Vidi Copy Protection System for the DVD+R/+RW Video Recording Format or reliance on the accuracy of this document.

LICENSING

Application of the System Description Vidi Copy Protection System for the DVD+R/+RW Video Recording Format in both disc and equipment products requires a separate license from Philips.

CLASSIFICATION

The information contained in this document is marked as non-confidential.

NOTICE

For any further explanation of the contents of this document, or in case of any perceived inconsistency or ambiguity of interpretation, or for any information regarding the Vidi Copy Protection System for the DVD+R/+RW Video Recording Format patent license program, please consult:

Royal Philips Electronics
Intellectual Properties & Standards
Business Support
Building WAH
P.O. Box 220
5600 AE Eindhoven
The Netherlands

Fax: +31 - 40 - 27 32113
Internet: http://www.licensing.philips.com/
E-mail: info.licensing@philips.com

Table of Contents

List of Figures

List of Tables

1. General

1.1 Scope

The System Description Vidi defines a method to prevent unauthorized copying and/or redistribution of video data that is recorded in the DVD+R/+RW Video Recording Format. The Vidi copy protection features are triggered by control information contained in video data incoming to a Vidi-enabled video recorder. Copy protection is achieved by cryptographically binding the recorded video data to the physical media. For that purpose, Vidi-enabled video recorders as well as Vidi-enabled video players use licensable secrets and technologies.

1.2 Main features

Robust copy protection system that includes the following features:

- Encryption of the recorded video data using strong cryptography (AES).
- Randomly generated Unique ID to bind the recorded video data to the physical media.
- Authorization of individual devices to provide recovery from potential security breaches.
- Intergrity protection of copy and redistribution control information contained in the recorded video data.
- Compatibility of discs that support Vidi protected recordings with existing DVD+R/+RW equipment.[1]
- Low impact on design and manufacture of Vidi-enabled equipment and media.

1.3 References and conformance

All specifications in this document are mandatory, unless specifically indicated as recommended or optional or informative. In addition to the specifications provided in this document, Vidi also conforms to the applicable parts of the International Standards or System Descriptions listed below:

CBC	Recommendation for Block Cipher Modes of Operation: Methods and Techniques, NIST Special Publication 800-38A, December 2001.
DVD+R	System Description DVD+R 4.7 Gbytes, Basic Format Specifications.
DVD+R DL	System Description DVD+R 8.5 Gbytes, Basic Format Specifications.
DVD+RW	System Description DVD+RW 4.7 Gbytes, Basic Format Specifications.
DVD+VR	System Description DVD+RW 4.7 Gbytes, Video Format Specifications.
DVD-ROM	DVD Specifications for Read-Only Disc, Part 1, Physical Specifications.
DVD-Video	DVD Specifications for Read-Only Disc, Part 3, Video Specifications.
FIPS 140-1	Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication (FIPS PUB) 140-1.
FIPS 197	Advanced Encryption Standard, Federal Information Processing Standards Publication (FIPS PUB) 197.
ISO 646	Information technology — ISO 7-bit coded character set for information interchange, Ref. No. ISO/IEC 646:1991.
MMC-4	SCSI Multi-Media Commands – 4 (T10/1545D).

[1] However, Vidi protected recordings do not play on existing DVD+R/+RW equipment.

1.4 Definitions

ADIP	Address In Pre-groove. The addressing method used on a blank disc. See [DVD+RW], Section 14, Track format, and [DVD+R], Section 14, Track format, and [DVD+R DL], Section 14, Track format.
AES	Advanced Encryption Standard. The block cipher that is used for encryption and decryption.
AKB	Application Key Block. An EKB structure that is embedded in an Application for the purpose of authenticating with a Drive.
Application	A software function or a hardware function that has the purpose of formatting or rendering Protected Video Recordings.
APS	Analog Protection System. A method of embedding copy management information in an analog video signal.
Audio Pack	A data structure containing audible data. See [DVD-Video], Section 5.2.4, Audio pack (A_PCK), and [DVD+VR], Section 3.4.3, IEC-60958 Audio packs (IEC_PCK).
Authorization Key	A cryptographic key that is carried by a leaf node of an EKB structure.
AV Pack	A Video Pack, an Audio Pack, a Sub-Picture Pack, or a User Defined Pack.
AV Sector	2048 Bytes of data according to the Protected Video Format.
BP	Byte Position. The location of a byte in a sequence of bytes.
Buffer Zone 2	The last 512 sectors of the Lead-in on a DVD+R/+RW disc. See [DVD+RW], Section 17.12, Buffer Zone 2, and [DVD+R], Section 18.9, Buffer Zone 2, and [DVD+R DL], Section 18.9, Buffer Zone 2.
Bus Key	A cryptographic key that is shared by an Application and a Drive as a result of the Drive to Application (Host) authentication protocol.
CBC	Cipher Block Chaining. An encryption mode that is used for data exceeding the AES block size.
CCI	Copy Control Information. A collection of status bits (such as APS, CGMS, and/or EPN) contained in video data that indicates if it is permitted to redistribute and/or make a copy of all or part of the video data.
CGMS	Copy Generation Management System. A method of embedding copy management information in a digital video signal.
CDB	Command Descriptor Block. A data structure that contains a SCSI Multi-Media Command.
Data Frame	The main data contained in a sector, extended with sector header data. See [DVD+RW], Section 13.1, Data Frames, and [DVD+R], Section 13.1, Data Frames, and [DVD+R DL], Section 13.1, Data Frames.
Data Zone	An area on a DVD+R/+RW disc that contains one or more Protected Video Recordings, and optionally other data. See [DVD+RW], Section 18, Data Zone, and [DVD+R], Section 19, Data Zone, and [DVD+R DL], Section 19, Data Zone.
Device ID	A 40-bit binary string that identifies a Player or a Recorder.

Disc	A DVD+R/+RW disc that indicates support for Protected Video Recordings. This indication is contained in the Physical Format Information.
Disc Key	A cryptographic key that is obtained from hashing the Root Key and the Unique ID. The Disc Key is used to protect the Unique Key.
DKB	Disc Key Block. An EKB structure contained on a Disc, which authorizes Players and Recorders to record or render Protected Video Recordings.
Drive	A DVD+R/+RW playback or recording device that combines with a Host or a hardware Application to form a Player or a Recorder.
ECC Block	Error Correction Code Block. A sequence of 16 sectors for which an error correction mechanism is defined. See [DVD+RW], Section 13.3, ECC Blocks, and [DVD+R], Section 13.3, ECC Blocks, and [DVD+R DL], Section 13.3, ECC Blocks.
EKB	Enabling Key Block. A data structure that authorizes Vidi system components. See also AKB and DKB.
EPN	Encryption Plus Non-assertion. A method of embedding redistribution control data in a broadcast digital video signal.
Extended Format Information	Format information pertaining to Vidi that is contained on a blank Disc. The Extended Format Information is contained in the AUX bytes of the ADIP words in the Data Zone and/or in the Initial Zone in the main data channel.
Host	A general-purpose, open computing platform that runs a software Application.
Initial Zone	The first part of the Lead-in on a DVD+RW disc; the first part of the Inner Drive Area on a DVD+R disc. See [DVD+RW], Section 17.1, Initial Zone, and [DVD+R], Section 17.1, Initial Zone, and [DVD+R DL], Section 17.1, Initial Zone.
Initialization Vector 1	A 128-bit licensed constant that is used in CBC-mode encryption and decryption of AV Packs.
Initialization Vector 2	A 128-bit licensed constant that is used in the Drive to Application (Host) authentication protocol.
Lead-in	An area on a DVD+R/+RW disc that precedes the Data Zone. See [DVD+RW], Section 17, Lead-in Zone, and [DVD+R], Section 18, Lead-in Zone, and [DVD+R DL], Section 18, Lead-in Zone.
MAC	Message Authentication Code. A cryptographic code that is used to verify that a message has not been tampered with.
Navigation Pack	A data structure containing presentation control information, data search information, and real-time data information. See also [DVD-Video], Section 5.2.2, Navigation pack (NV_PCK), and [DVD+VR], Section 3.4.1, PCI_GI Extension.
Node Key	One of a set of secret cryptographic keys that is associated with a Device ID. A Node Key is associated with a bit position of the Device ID.
Physical Address	The address information in an ADIP word. See [DVD+RW], Section 14.4.1.1, ADIP word structure, and [DVD+R], Section 14.4.1.1, ADIP word structure, and [DVD+R DL], Section 14.4.1.1, ADIP word structure.

Physical Format Information
: Auxiliary information about the disc contained in the ADIP, as defined in [DVD+RW], Section 14.4.2, Physical format information in ADIP, and in [DVD+R], Section 14.4.2, Physical format information in ADIP, and in [DVD+R DL], Section 14.4.2, Physical format information in ADIP.

Physical Sector Number.
: Bit 0 through 23 of the ID field of a Data Frame. See [DVD+RW], Section 13.1.1, Identification Data (ID), and [DVD+R], Section 13.1.1, Identification Data (ID), and [DVD+R DL], Section 13.1.1, Identification Data (ID).

Player
: A DVD+R/+RW video playback function capable of rendering video stored according to the Protected Video Format. A Player may consist of a Drive/Host combination.

Program Key
: A cryptographic key that is used to compute the Sector Keys of a Protected Video Recording. Multiple Program Keys may be used within a single Protected Video Recording.

Protected Video Format
: The data structures specified in [DVD-Video] plus [DVD+RW] plus this System Description Vidi.

Protected Video Recording
: A recording of moving pictures, which is structured according to the Protected Video Format.

Recorder
: A DVD+R/+RW video recording function capable of storing video according to the Protected Video Format. A Recorder is also a Player. A Recorder may consist of a Drive/Host combination.

Root Key
: A cryptographic key, which is contained in an EKB structure in an encrypted form.

Sector Key
: A cryptographic key that is used to encrypt the content of an individual sector that contains part of a Protected Video Recording.

Sub-picture Pack
: A data structure containing still picture data. See also [DVD-Video], Section 5.2.5, Sub-picture pack (SP_PCK).

Unique ID
: A 40-bit binary string that identifies a Disc.

Unique Key
: A cryptographic key that is used to protect the Program Key.

User Defined Pack
: A data structure containing under defined data. See also [DVD+VR], Section 3.4.2, User Defined pack (UD_PCK).

Video Pack
: A data structure containing moving picture data. See also [DVD-Video], Section 5.2.3, Video pack (V_PCK).

Video Recording Format
: The data structures specified in [DVD-Video] plus [DVD+VR].

Vidi
: The Vidi Copy Protection System for the DVD+R/+RW Video Recording Format as described in the System Description Vidi (this document).

VOB
: Video Object. See [DVD-Video], Section 5, Video Object (VOB).

1.5 Conventions

1.5.1 Bit ordering

The graphical representation of all multiple-bit quantities is such that the most significant bit (msb) is on the left, and the least significant bit (lsb) is on the right. Figure 1-1 defines the bit position in a byte.

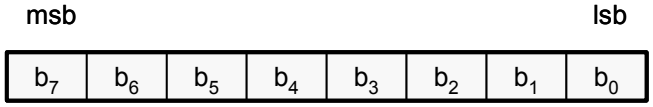

Figure 1-1: Bit ordering in a byte

1.5.2 Byte numbering

The bytes in a sequence of *n* bytes are located at byte positions 0..*n* – 1. Byte position 0 corresponds to the lowest address; byte position *n* – 1 corresponds to the highest address.

1.5.3 Bit sequence

In all places where a bit sequence is used, a most significant bit first notation is used. Bit sequences are enclosed between single quotes (‘’).

1.5.4 Decimal notation

All decimal values are preceded by a blank space or by the range indicator (..) when included in a range. The most significant digit is on the left; the least significant digit is on the right.

1.5.5 Hexadecimal notation

Unless indicated otherwise, all hexadecimal values are preceded by “0x”. The most significant nibble is on the left; the least significant nibble is on the right.

1.6 Operators

1.6.1 Range indicator

The symbol “..” indicates a range of integer values. The difference between each adjacent pair of values in the range is 1. Both the values represented by the left-hand operator and the right-hand operator are included in the range.

1.6.2 Bit string concatenation

The symbol “||” indicates concatenation of two bit strings. In the resulting bit string, the most significant bit of the right-hand operand directly follows the least significant bit of the left-hand operand.

1.6.3 Bit wise exclusive-OR

The symbol “⊕” indicates a bit wise exclusive-OR operation of its left-hand and right-hand operands.

1.6.4 Addition

The symbol “+” indicates addition of its left-hand and right-hand operands.

1.6.5 Multiplication

The symbol “*” indicates multiplication of its left-hand and right-hand operands.

1.6.6 Division

The symbol “/” indicates integer division of its left-hand operand (the dividend) and its right-hand operator (the divisor). Any fractional result shall be truncated towards zero.

This page is intentionally left blank.

2. System Overview (Informative)

2.1 General

The System Description Vidi, in short “Vidi,” defines a method for preventing unauthorized copying and/or redistribution of video data that is recorded in the DVD+R/+RW Video Recording Format. Examples of video data that require the use of the Vidi copy protection features are the following:

- Video data asserting that only one generation of copies is permitted. Such video data typically reaches a Recorder through a protected channel, such as DTCP (Digital Transmission Content Protection; for more information see http://www.dtcp.com).
- Publicly broadcast television signals asserting that redistribution is not authorized.

Usage of the Vidi copy protection features requires special DVD+R/+RW discs. Such special discs are fully compatible with DVD+R/+RW players and recorders that do not implement Vidi.

At the basis of the Vidi copy protection features is encryption of the recorded video data using strong cryptography. Vidi uses a standard cipher (AES) that has a 128-bit key. Every 2048-byte sector on a disc that contains protected video data is encrypted using its own unique Sector Key. For convenient navigation in an encrypted video recording, the first 128 byes of a sector containing video header information are not encrypted.
Encryption of the video data is not sufficient to prevent copying. For this purpose, a Recorder randomly generates a 40-bit Unique ID, which uniquely identifies a Disc. The Recorder stores this Unique ID on the Disc in a location so as to minimize the risk that DVD+R/+RW recorders that do not implement Vidi overwrite the Unique ID. The function of the Unique ID is to bind the encrypted video data to the physical media. For that purpose, the Unique ID serves as an ingredient for the calculation of the Sector Keys. This ensures that decryption can be performed only if the encrypted video data is read from the Disc used for the original recording.
As with any system that uses cryptography to protect information, Vidi relies on a number of secret keys. Each Player/Recorder contains a set of so-called Node Keys KN. All stand-alone Players/Recorders contain a unique set of Node Keys KN. Combined with a Disc Key Block (DKB), the set of Node Keys KN serves as another ingredient to the calculation of the Sector Keys. The DKB authorizes individual Players/Recorders or groups of Players/Recorders to render or record encrypted video data. Players/Recorders are authorized only if they are able to successfully decode the DKB using the set of Node Keys KN. In the event that one or more Node Keys KN become public knowledge, the DKB will be modified so as to remove the authorization of the Player(s)/Recorder(s) that use those Node Keys KN. This means that those Player(s)/Recorder(s) cannot use Discs that contain the modified DKB to render or record encrypted video data. Recording or rendering of unencrypted video data remains possible at all times.
The DKB is stored in the ADIP and/or is pre-recorded on the Disc. It is the responsibility of the Recorder to copy the DKB to a location on the Disc that is accessible to Players. In order to prevent tampering with the DKB, the Recorder must check the copied DKB using the DKB hash value that is stored in the ADIP.
The encrypted video data typically contains Copy Control Information (CCI) in the (unencrypted) portion of a sector. To prevent tampering with the CCI, Navigation Packs in the encrypted video data contain an encrypted copy of the CCI. A Player must check the consistency of the unencrypted CCI and the encrypted copy of the CCI. In case of an inconsistency, the Player must apply the most restrictive copy of the CCI while decrypting and rendering the video data.

2.2 Computer environments

In a computer environment, a Player/Recorder consists of a Drive and a software Application. In this combination, the software Application calculates the Sector Keys and handles decryption/encryption of the video data. For this purpose, the software Application contains a set of Node Keys KN_h. Unlike in stand-alone Players/Recorders, individual installations of a software Application may contain the same set of Node Keys KN_h. In addition, the software Application handles the integrity protection of the CCI provided by the encrypted copy of the CCI in the Navigation Packs. The Drive generates the Unique ID and stores the Unique ID on the Disc. In addition, a Drive that has recording functionality reads the DKB hash value from the ADIP, and writes the DKB to a location that is accessible for a Drive that has playback-only functionality (Buffer Zone 2 in the Lead-in).
In order to calculate the Sector Keys, the software Application must retrieve both the Unique ID and the DKB hash value after authenticating the Drive. For this purpose, software Applications contain a built-in Application Key Block (AKB), while Drives contain a set of Node Keys KN_d. As part of the authentication protocol, the Application decodes the AKB using its Node Keys KN_h, while the Drive decodes the AKB using its Node Keys KN_d. Only if both the Application and the Drive are authorized, the authentication protocol results in a so-called Bus Key KB. The Bus Key KB is used to encrypt the Unique ID and the DKB hash value, over the interface between the Drive and the software Application. This ensures that the software Application obtains the Unique ID and the DKB hash value from the physical media, i.e. the Disc. The significance thereof is that the software Application ensures that encrypted video data is bound to that particular Disc.

3. Cryptographic Functions

3.1 Encryption algorithm

The encryption algorithm shall be AES, as specified in [FIPS 197] in 128-bit key mode. Figure 3-1 schematically shows AES encryption.

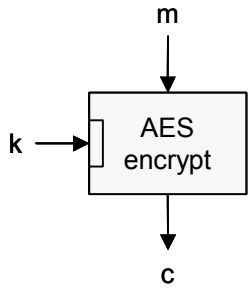

Figure 3-1: AES encryption

Encryption is denoted as c = AESEncrypt(k, m), where k is a 128-bit key, and m is the 128-bit plain text block to be encrypted. The result is a 128-bit cipher text block c.

3.1.1 CBC-mode encryption

Figure 3-2 shows Cipher Block Chaining (CBC) mode encryption of multiple plain text blocks, as specified in [CBC]. All data paths shown in Figure 3-2 are 128 bits wide.

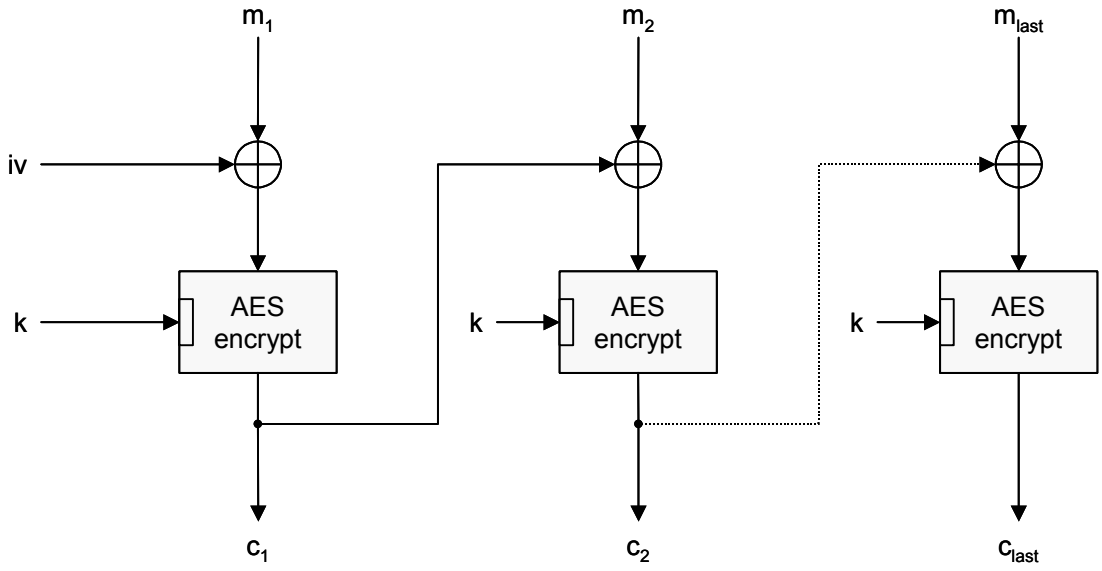

Figure 3-2: CBC-mode encryption

CBC-mode encryption is denoted as c = AESCBCEncrypt(k, iv, m), where k is a 128-bit key, iv is a 128-bit initialization vector, and m is a sequence of two or more consecutive 128-bit plain text blocks m_i, i = 1..last. The result is a sequence c of consecutive cipher text blocks c_i, i = 1..last, which shall be calculated from the equations

$c_0 = iv$;
c_i = AESEncrypt(k, $m_i \oplus c_{i-1}$), i = 1..last.

3.2 Decryption algorithm

The encryption algorithm shall be AES, as specified in [FIPS 197] in 128-bit key mode. Figure 3-3 schematically shows AES decryption.

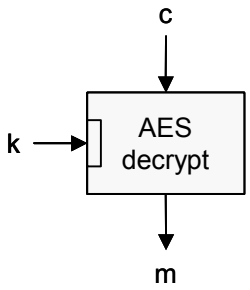

Figure 3-3: AES decryption

Decryption is denoted as m = AESDecrypt(k, c), where k is a 128-bit key, and c is the 128-bit cipher text block to be decrypted. The result is a 128-bit plain text block m.

3.2.1 CBC-mode decryption

Figure 3-4 shows CBC-mode decryption of multiple cipher text blocks, as specified in [CBC]. All data paths shown in Figure 3-4 are 128 bits wide.

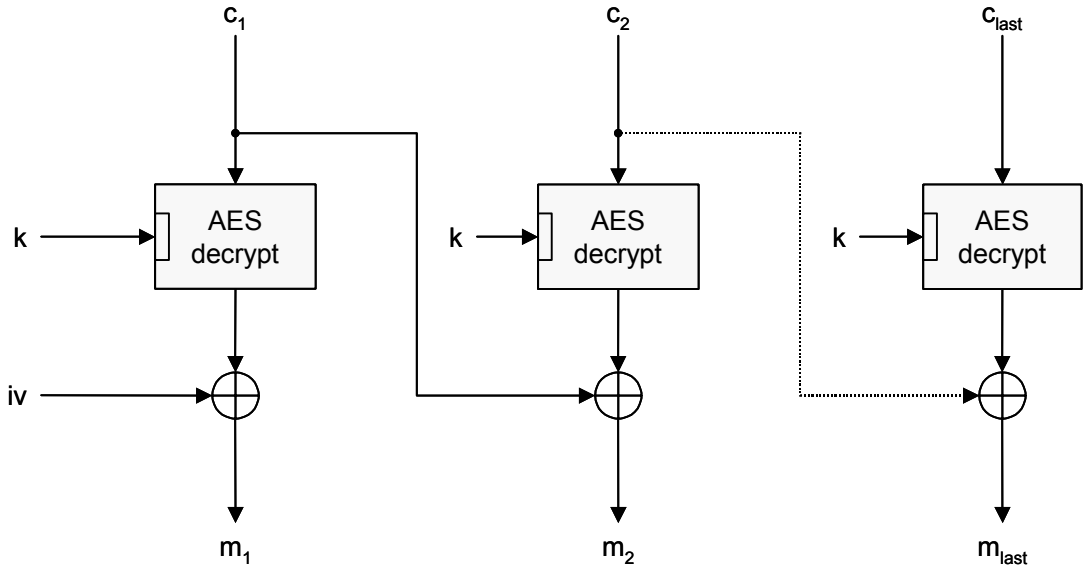

Figure 3-4: CBC-mode decryption

CBC-mode decryption is denoted as m = AESCBCDecrypt(k, iv, c), where k is a 128-bit key, iv is a 128-bit initialization vector, and c is a sequence of two or more consecutive 128-bit cipher text blocks c_i, i = 1..last. The result is a sequence m of consecutive plain text block m_i, i = 1..last, which shall be calculated from the equations

$c_0 = iv$;
m_i = AESDecrypt(k, c_i) $\oplus$ c_{i-1}, i = 1..last.

3.3 Hash algorithm

Figure 3-5 shows the hash algorithm. All data paths shown in Figure 3-5 are 128 bits wide.

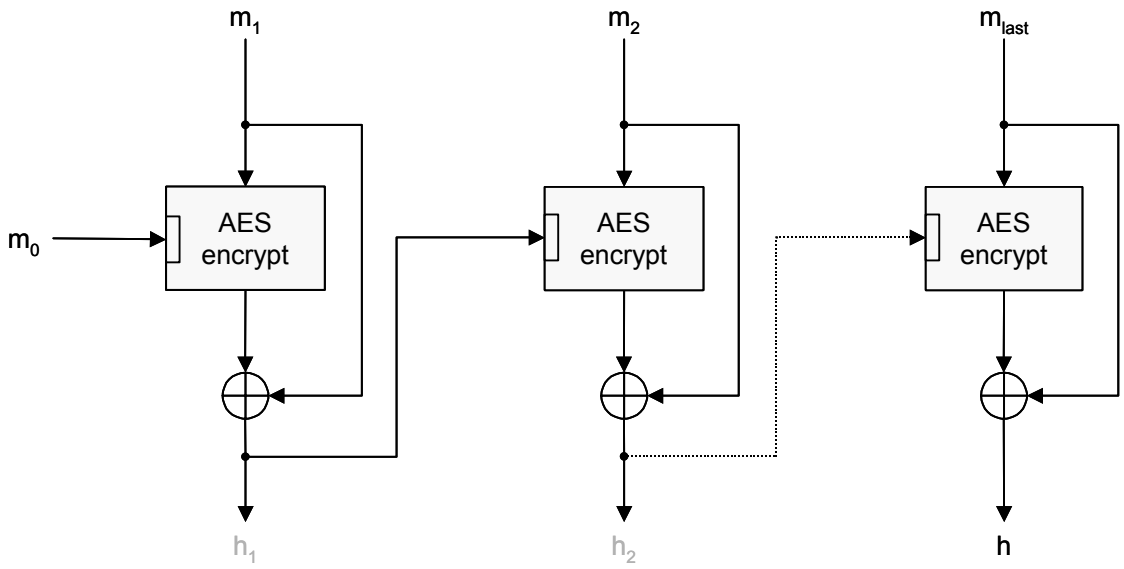

Figure 3-5: Hash function

Hashing is denoted as h = AESHash(m), where m is a sequence of 17 or more bytes. The sequence m shall be padded at the end by the shortest amount of zeros (bytes of value 0x00), such that m consists of two or more consecutive 128-bit blocks m_i, i = 0..last. The result is a single 128-bit value h, which shall be calculated from the equations

$h_1 = \text{AESEncrypt}(m_0, m_1) \oplus m_1$;
$h_i = \text{AESEncrypt}(h_{i-1}, m_i) \oplus m_i$, $i = 2..\text{last} - 1$;
$h = \text{AESEncrypt}(h_{\text{last}-1}, m_{\text{last}}) \oplus m_{\text{last}}$.

All intermediate values h_i shall be discarded.

3.4 Random number generator

Figure 3-6 schematically shows the random number generator.

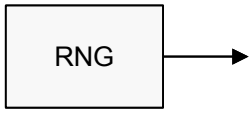

Figure 3-6: Random number generator

The random number generator shall either be a true random number generator, or a pseudo-random number generator that passes the Monobit Test and the Poker Test and the Runs Test and the Long Run Test defined in [FIPS 140-1], Section 4.11.1.

This page is intentionally left blank.

4. Content Encryption and Decryption

4.1 Overview (normative)

Figure 4-1 provides a schematic diagram of the encryption and decryption system for Protected Video Recordings. The dotted box on the left part of Figure 4-1 shows the encryption and decryption steps that a Recorder shall execute in the case that the Disc already contains one or more Protected Video Recordings. Section 4.2.1 provides a detailed explanation of these steps as well as the additional steps that a Recorder shall execute in order to make the first Protected Video Recording on a blank Disc. The shaded oval in the center part of Figure 4-1 represents the Disc containing the data that is required to execute the encryption and decryption steps. The dotted box on the right part of Figure 4-1 shows the decryption steps that a Player shall execute. Section 4.3.1 provides a detailed explanation of these steps. Unless indicated otherwise, all data paths in Figure 4-1 are 128 bits wide. A Player as well as a Recorder contain a 40-bit Device ID and set of 40 Node Keys KN (see Section 5). The size of the DKB is *N* bytes (see Section 5.4).

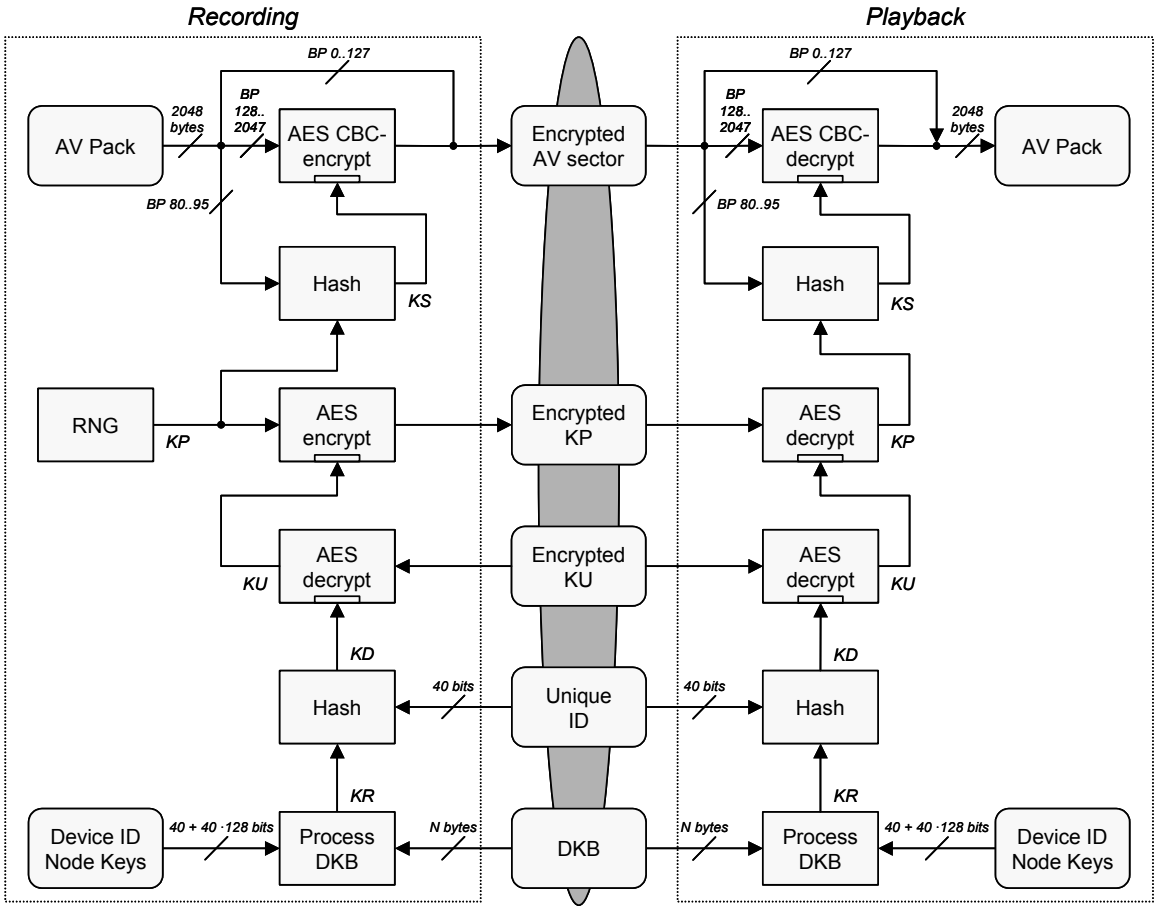

Figure 4-1: Schematic diagram of the key hierarchy

4.2 Recording

4.2.1 Encryption system

This Section 4.2.1 provides an explanation of the encryption steps that a Recorder shall execute to make a Protected Video Recording.

DKB. The Recorder shall ensure that Buffer Zone 2 contains a valid copy of the DKB. See also Section 5 and Section 6.3.3. For this purpose, the Recorder shall execute either of the following two actions:

- Copy the DKB from the Data Zone ADIP or from the Initial Zone to Buffer Zone 2. See also Section 6.2.1 and Section 6.3.1.
- Calculate

  DKB Hash = AESHash(DKB),

  where DKB is retrieved from Buffer Zone 2. Verify that DKB Hash is equal to the DKB hash value contained in the Data Zone ADIP (see Section 6.2.2). If DKB Hash is not equal to the DKB hash value contained in the Data Zone ADIP, the Recorder shall execute either of the following actions:
  - Copy the DKB from the Data Zone ADIP or from the Initial Zone to Buffer Zone 2. See also Section 6.2.1 and Section 6.3.1.
  - Inform the user that Protected Video Recordings are not possible on this Disc.

Root Key KR. The Recorder shall process the DKB using its Device ID and Node Keys KN (see Section 5.2). If the Recorder is authorized to make Protected Video Recordings on the Disc, processing of the DKB yields the 128-bit Root Key KR.

Unique ID. The Recorder shall ensure that Buffer Zone 2 contains a valid Unique ID. For this purpose, the Recorder shall execute either of the following two actions:

- Generate a non-zero 40-bit Unique ID using a random number generator. The Recorder shall store the generated Unique ID in all Data Frames in Buffer Zone 2 that contain the DKB (see also Section 6.3.2).
- Read the Unique ID from Buffer Zone 2, and verify that the Unique ID is non-zero. If all bits of the Unique ID are zero, the Recorder shall not make a Protected Recording on the Disc.

Disc Key KD. Using the Root Key KR and the Unique ID, the Recorder shall compute a 128-bit Disc Key KD as follows:

KD = AESHash(KR || Unique ID).

Unique Key KU. When using a Disc that does not contain Protected Video Recordings, the Recorder shall generate a 128-bit Unique Key KU using a random number generator (RNG). The Recorder shall use the Disc Key KD to encrypt the Unique Key KU as follows:

encrypted KU = AESEncrypt(KD, KU).

The Recorder shall store the encrypted Unique Key KU on the Disc in the file Video_RM.IFO (see also Section 6.4.2).
When using a Disc that contains one or more Protected Video Recordings, the Recorder shall retrieve the encrypted Unique Key KU from the Disc (see also Section 6.4.2). Next, the Recorder shall use the Disc Key KD to decrypt the encrypted Unique Key KU as follows:

KU = AESDecrypt(KD, encrypted KU).

Program Key KP. The Recorder shall generate a 128-bit Program Key KP using a random number generator (RNG). The Recorder shall generate a new Program Key KP if any of the following conditions apply:

- The Recorder starts a new video recording according to the Protected Video Format.
- The CCI status of the incoming video data changes (see also Section 4.2.2).
- Whenever the Recorder deems necessary.

Notwithstanding the above conditions, the Recorder shall not change the Program Key KP more often than once every 10 seconds of real time video.
The Recorder shall use the Unique Key KU to encrypt the Program Key KP as follows:

encrypted KP = AESEncrypt(KU, KP).

The Recorder shall store the encrypted Program Key KP on the Disc (see also Section 6.4.1).

Sector Key KS. The Recorder shall use the Program Key KP to compute a 128-bit Sector Key KS as follows:

KS = AESHash(KP || BP 80..95).

Here BP 80..95 represents byte positions 80 through 95 (128 bits) of the unencrypted 2048-byte AV Sector.

AV Pack. The Recorder shall encrypt all AV Packs in the Protected Video Recording (see Section 4.2.2). The Recorder shall use the PES Scrambling Control field in the AV Pack to indicate that the AV Pack stored on the Disc is encrypted (see Section 6.4.3). In addition, the Recorder shall set the Stream ID field in the encrypted AV Pack to the value specified in Section 6.4.3.[2] The Recorder shall use the Sector Key KS to encrypt the selected AV Pack as follows:

encrypted AV Sector = BP 0..127 || AESCBCEncrypt(KS, IV1, BP 128..2047).

Here BP 0..127 represents byte positions 0 through 127 (128 bytes) of the unencrypted AV Pack. The Recorder shall not encrypt these bytes. BP 128..2047 (1920 bytes) represents byte positions 128 through 2047 of the unencrypted AV Pack. The Recorder shall encrypt these bytes in CBC mode. The initialization vector IV1 is a 128-bit licensed constant.

4.2.2 Copy Control Information insertion

Copy Control Information shall be inserted into the Protected Video Recording according to the compliance rules given in the “Vidi Content Protection Agreement.”

[2] This avoid playback problems on video players that do not support Vidi protected recordings.

4.3 Playback

4.3.1 Decryption system

This Section 4.3.1 provides an explanation of the decryption steps that a Player shall execute to render a Protected Video Recording.

Root Key KR. The Player shall process the DKB using its Device ID and Node Keys KN (see Section 5.2). If the Player is authorized to render Protected Video Recordings that are contained on the Disc, processing of the DKB yields the 128-bit Root Key KR.

Disc Key KD. Using the Root Key KR and the Unique ID, the Player shall compute a 128-bit Disc Key KD as follows:

KD = AESHash(KR || Unique ID).

Unique Key KU. The Player shall retrieve the encrypted Unique Key KU from the Disc (see also Section 6.4.2). Next, the Player shall use the Disc Key KD to decrypt the encrypted Unique Key KU as follows:

KU = AESDecrypt(KD, encrypted KU).

The size of the Unique Key KU is 128 bits.

Program Key KP. The Player shall use the Unique Key KU to decrypt the encrypted Program Key KP as follows:

KP = AESDecrypt(KU, encrypted KP).

The size of the Program Key KP is 128 bits.

Sector Key KS. The Player shall read a sector from the Disc. If the sector is encrypted (see also Section 6.4.3), the Player shall use the Program Key KP to obtain a 128 bit Sector Key KS as follows:

KS = AESHash(KP || BP 80..95).

Here BP 80..95 represents byte positions 80 through 95 (128 bits) of the encrypted AV Sector.

AV Pack. If the AV Pack in a sector is encrypted (see also Section 6.4.3), the Player shall use the Sector Key to decrypt the AV Pack as follows:

AV Pack = BP 0..127 || AESCBCDecrypt(KS, IV1, BP 128..2047).

Here BP 0..127 represents byte positions 0 through 127 (128 bytes) of the encrypted AV Sector. The Player shall not decrypt these bytes. BP 128..2047 (1920 bytes) represent byte positions 128 through 2047 of the encrypted AV Sector. The Player shall decrypt these bytes in CBC mode. The initialization vector IV1 is a 128-bit licensed constant. After decryption, the Player may change the PES Scrambling Control field and the Stream ID field to values defined for plain text AV Packs (see Section 6.4.3).

4.3.2 Copy Control Information verification

While rendering a Protected Video Recording, the Player shall check that the CCI bits (see [DVD-Video] and [DVD+VR]) in the Protected Video Recording are consistent. If the CCI bits are not consistent, the Player shall use the most restrictive of the CCI bits while rendering the Protected Video Recording. In addition, the Player shall check that the CCI MAC contained in the Navigation Packs of the Protected Video Recording (see also Section 6.4.1) is correct and consistent with the unencrypted CCI in the Navigation Pack. If the CCI MAC is not correct and/or not consistent with the unencrypted CCI in the Navigation Pack, the Player shall use the most restrictive of the unencrypted CCI bits and the copy of the unencrypted CCI bits in the CCI MAC, while rendering the Protected Video Recording. Otherwise, the Player shall continue rendering of the Protected Video Recording. Note that the CCI MAC shall be deemed not correct if the Signature field of CCI Digest does not contain the value specified in Section 6.4.1. The Player shall obtain CCI Digest from the CCI MAC as follows:

CCI Digest = AESDecrypt(KP, CCI MAC).

5. Enabling Key Block

5.1 Overview (informative)

The Enabling Key Block (EKB) authorizes Players and Recorders to process encrypted content. Authorized Players and Recorders process the EKB to obtain the Root Key KR. Unauthorized, or revoked, Players and Recorders cannot obtain the Root Key KR from the EKB. The EKB is based on the broadcast encryption mechanism that is described in C.K. Wong, M. Gouda, S.S. Lam, Secure Group Communications Using Key Graphs, Technical Report TR 97-23, The University of Texas at Austin, July 1997, and in D.M. Wallner, E.J. Harder, and R.C. Agee, Key Management for Multicast: Issues and Architectures, Request For Comments 2627, June 1999.

5.2 Tree tracing

The EKB contains a representation of a binary tree structure. Figure 5-1 shows an example of the top part of such a tree structure. The white circles and the gray circles represent the nodes of the tree. The black circle represents the root node of the tree. The node directly above a node is called its parent. A node directly below a node is called its child. The two nodes that have the same parent are called siblings. A node that does not have any children is called a leaf. All nodes that are on the (single) path from a node up to the root are called its ancestors. All nodes that are on the (multiple) paths from a node down to the leaf nodes are called its descendants. The tree that is formed by a node and all of its descendants is called a sub-tree. In Figure 5-1 the white circles represent leaf nodes, and the gray circles represent parent nodes. The root node is at level 0 in the tree. The child nodes of a node at level *n* in the tree are at level *n* + 1 in the tree. The EKB contains the root node and at least one leaf node.

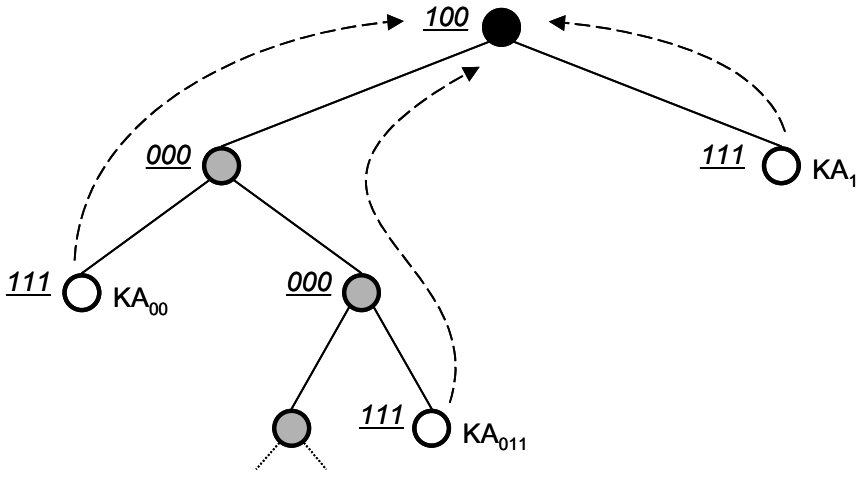

Figure 5-1: Example of the top part of an EKB tree

The nodes of the EKB tree contain the following information: a three-bit tag, and optionally an Authorization Key KA.

The tags describe the tree structure. Each node carries a tag. In Figure 5-1, the underlined bit sequences left to each node indicate the tags. The tag bits have the following meaning: The leftmost tag bit is set to '1' if the node is the root node or a leaf node; otherwise the leftmost tag bit is set to '0'. The center tag bit is set to '0' if the node has a left-hand child; otherwise the center tag bit is set to '1'. Likewise, the rightmost tag bit is set to '0' if the node has a right-hand child; otherwise the rightmost tag bit is set to '1'.

The Authorization Keys KA consist of the Root Key KR decrypted with the appropriate Node Keys KN (see below). Each leaf node carries a unique Authorization Key KA. Parent nodes do not carry an Authorization Key KA. In Figure 5-1, KA_x indicate the Authorization Keys. In this notation, the subscript *x* is a bit string that matches the most significant bits of one or more Device IDs (see below).

Players and Recorders are identified using a 40-bit Device ID. Each bit of the Device ID has an associated Node Key KN. The Node Key KN_0 that is associated with bit 0 of a Device ID is unique for that particular Device ID. The Node Key KN_1 that is associated with bit 1 of a Device ID is shared by two Device IDs (namely the Device IDs that become identical if bit 0 of those Device IDs is discarded). The Node Key KN_2 is shared by four Device IDs (namely the Device IDs become are identical if bit 0 and bit 1 of those Device IDs are discarded). In general, the Node Key KN_j is shared by 2^j Device IDs (namely the Device IDs that become identical if bits 0..*j* – 1 of those Device IDs are discarded).

Each Device ID is associated with a single leaf node in the EKB tree. Multiple Device IDs may be associated with a single leaf node. The following algorithm determines the leaf node that a Device ID is associated with:

- Start at the root node.
- For the appropriate number of Device ID bits, working from the most significant bit (bit 39) towards the least significant bit (bit 0), repeat the following steps in the order of appearance:
  - If the Device ID bit is a '0', proceed to the left-hand child node. If the left-hand child node does not exist, the Player or Recorder is not authorized. Further processing of the EKB will not yield the correct Root Key KR.
  - If the Device ID bit is a '1', proceed to the right-hand child node. If the right-hand child node does not exist, the Player or Recorder is not authorized. Further processing of the EKB will not yield the correct Root Key KR.
  - Stop if the node reached in the previous two steps is a leaf node.

The Player or Recorder shall use the Authorization Key KA, which is placed on the leaf node found by the above algorithm, to obtain the Root Key KR as follows:

$$KR = AESEncrypt(KN_j, KA_x).$$

In this notation, KN_j is the Node Key that is associated with bit position *j* of the Device ID, where *j* is the position of the Device ID bit last processed in the above leaf finding algorithm. KA_x is the Authorization Key that is placed on the leaf node found by the leaf finding algorithm. Note that the subscript *x* (a bit string of length 40 – *j*) matches the most significant bits of the Device ID processed by the leaf finding algorithm and represents the path taken through the EKB.

See also Annex C for a few detailed examples.

5.3 EKB usage

A Player and a Recorder that does not consist of a Drive/Host combination shall contain a single Device ID as well as an associated set of Node Keys KN. The Device ID uniquely identifies that Player or Recorder. The set of Node Keys KN is unique for that Player or Recorder and coupled to the Device ID. The Player or Recorder shall use the set of Node Keys KN to decode the Disc Key Block (DKB) for content encryption and decryption (see Section 4).
A Drive shall contain a single Device ID_d as well as an associated set of Node Keys KN_d. The Device ID_d uniquely identifies that Drive. The set of Node Keys KN_d is unique for that Drive and coupled to the Device ID_d. The Drive shall use the set of Node Keys KN_d to decode the Application Key Block (AKB) for authentication with an Application (see Section 7).
An Application shall contain a single Device ID_h as well as an associated set of Node Keys KN_h. The Device ID_h may be identical in all installations of a software Application. The set of Node Keys KN_h may be identical in all installations of a software Application (the set of Node Keys KN_h is coupled to the Device ID_h). The Device ID_h shall be unique in all hardware Applications. The set of Node Keys KN_h is unique in all hardware Applications and coupled to the Device ID_h. The Application shall use the set of Node Keys KN_h to decode the DKB for content encryption and decryption (see Section 4) as well as to decode the AKB for authentication with a Drive (see Section 7).

5.4 EKB format

The EKB consists of three parts, namely a header part that includes fields for identification and verification purposes; a tag part that contains the tags that describe the EKB tree structure; and a key part that contains the Authorization Keys KA. Table 5-1 defines the format of the EKB. The header part extends from byte 0 through byte 287. The tag part extends from byte 288 through byte *M* – 1 (see below for the definition of *M*). The key part extends from byte *M* through the end of the EKB (byte *N* – 1; see below for the definition of *N*).

Byte \ Bit	7	6	5	4	3	2	1	0
0 : 3	EKB Size							
4 : 7	(msb) Sequence Number (lsb)							
8 : 31	(msb) Key Check Data (lsb)							
32 : 159	(msb) Authentication Data (lsb)							
160 : 287	Reserved							
288 289	(msb) Tag Count (lsb)							
290	Tag #1			Tag #2			Tag…	
:	…#3	…						
M – 1					Padding			
M : *N* – 1	(msb) Authorization Key #1 (lsb) (msb) Authorization Key #2 (lsb) …							

Table 5-1: EKB format

EKB Size. The size in bytes of the EKB (equal to *N*). The maximum size of the EKB is 448 kB.

Sequence Number. EKBs are issued as an ordered series. Each time the authorization of one or more Players and/or Recorders are removed, i.e. revoked, the Sequence Number of the EKB is incremented by one. The EKB that authorizes all Players and Recorders has Sequence Number 1.

Key Check Data. A Player and/or a Recorder may verify the correctness of the Root Key KR obtained from the EKB (according to the algorithm defined in Section 5.2) by executing the following steps

- Encrypt bytes 16..31 of the EKB (i.e. the 16 least significant bytes of Key Check Data) using the Root Key KR.
- If bytes 8..11 of the resulting encrypted block contain a copy of the Sequence Number, the Root Key KR is correct. Otherwise, the Root Key KR is not correct. In that case the Player or Recorder is not authorized. Note that a Player and/or a Recorder shall ignore bytes 0..7 and bytes 12..15 of the encrypted block.

A Player and/or a Recorder shall ignore bytes 8..15 of the EKB.

Authentication Data. Players and Recorders shall ignore this field.

Reserved. All reserved bytes are set to 0x00.

Tag Count. The tag part contains the (three-bit) tags carried by the nodes of the EKB tree. The Tag Count field contains the number of tags that follow in the remainder of the tag part. The tags are packed into bytes as shown in Table 5-1. If necessary, the last byte of the tag part is padded with zeros. The position $M - 1$ of the last byte of the tag part is calculated using the equation

$$M - 1 = 290 + (\text{Tag Count} * 3) / 8.$$

The tags are stored in a left-to-right, top-down structure, i.e. the tag of the root node comes first, then the tag(s) of the nodes at level 1, subsequently the tag(s) of the nodes at level 2, and so on, down to the tag(s) of the nodes at the lowest level.

Tag #*n*. The leftmost tag bit is set to ‘1’ if the node is the root node or a leaf node; otherwise the leftmost tag bit is set to ‘0’. The center tag bit is set to ‘1’ if the node does not have a left-hand child; otherwise the center tag bit is set to ‘0’. The rightmost tag bit is set to ‘1’ if the node does not have a right-hand child; otherwise the rightmost tag bit is set to ‘0’.

Padding. If necessary, padding bits are inserted to complete the last byte of the tag part. All padding bits are set to ‘0’.

Authorization Key #*n*. The key part contains the Authorization Keys KA carried by the leaf nodes of the EKB tree. The Authorization Keys KA are stored in a left-to-right, top-down structure, i.e. the Authorization Key(s) KA of level 1 come first, then the Authorization Key(s) KA of level 2, and so on, down to the Authorization Key(s) KA of the last level. The number of Authorization Keys KA contained in the key part is one less than the number of tags that have the leftmost tag bit set to ‘1’ (because the root node does not carry an Authorization Key KA). The position $N - 1$ of the last byte of the key part is calculated using the equation

$$N - 1 = M - 1 + 16 * \text{number of Authorization Keys KA in key part.}$$

6. Disc Format

6.1 Overview (informative)

The underlying physical format of the Disc is according to [DVD+RW] or [DVD+R] or [DVD+R DL]. The System Description Vidi provides extensions to this underlying physical format in three areas, namely the ADIP, the Lead-in, and the Data Zone.

6.2 ADIP

This Section 6.2 defines Vidi Extended Format Information. Extended Format Information is not defined in [DVD+RW], [DVD+R], and [DVD+R DL], but will be included in an upcoming release of the DVD+R/+RW basic format specifications. See also Annex F.
Vidi defines two data blocks that shall occur in the Extended Format Information: A Disc shall contain one or more regions that contain the DKB (see Section 6.2.1). In addition, a Disc shall contain one or more regions that contain the DKB hash value (see Section 6.2.2).

6.2.1 DKB region descriptor

The EFI TOC on a Disc shall contain one or more DKB region descriptors. A DKB region that is contained in the AUX bytes of the ADIP in the Data Zone shall containone or more consecutive copies of the DKB as defined in Table 6-1. For the format of a DKB region that is contained in the main data channel see Section 6.3.1.The following fields of the DKB region descriptor shall have the values specified: The Region Type Identifier shall be set to 0x444B42 (the encoding of the characters “DKB” according to [ISO 646]); the Version Number shall be set to 0x00; and the Private bit shall be set to ‘0’.

<table>
<tr><th>Bit
Byte</th><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th><th>0</th></tr>
<tr><td>0
:
N – 1</td><td colspan="8">DKB #1</td></tr>
<tr><td>:</td><td colspan="8">:</td></tr>
<tr><td>N * (n – 1)
:
(N * n) – 1</td><td colspan="8">DKB #n</td></tr>
</table>

Table 6-1: DKB region

DKB #*n*. An EKB structure as defined in Section 5.4. *N* is the size of the DKB (in bytes), as defined in Table 5-1. The number *n* of copies of the DKB contained in the DKB region is contained in the corresponding Region Descriptor.

6.2.2 Hash region descriptor

The EFI TOC on a Disc shall contain one or more hash region descriptors. A hash region shall contain one or more consecutive copies of the hash of the DKB, as defined in Table 6-2. The hash region shall be stored in the AUX data bytes of the ADIP in the Data Zone. The following fields of the hash region descriptor shall have the values specified: The Region Type Identifier shall be set to 0x485348 (the encoding of the characters “HSH” according to [ISO 646]); the Version Number shall be set to 0x00; the Data Block Size shall be set to 16; the Private bit shall be set to ‘0’; and the Alternative Location shall be set to zero.

Bit / Byte	7	6	5	4	3	2	1	0
0	DKB Hash #1							
:								
15								
:	:							
16 * (*n* – 1)	DKB Hash #*n*							
:								
(16 * *n*) – 1								

Table 6-2: Hash region

DKB Hash #*n*. The hash value of the DKB calculated as

DKB Hash = AESHash(DKB),

where DKB is the EKB structure as defined in Table 5-1. The number *n* of copies of the DKB Hash contained in the hash region is contained in the corresponding Region Descriptor.

6.3 Lead-in / Inner Drive Area

This Section 6.2.2 provides extensions to [DVD+RW], Section 13.1.3, RSV, Section 17.1, Initial Zone, and Section 17.12, Buffer Zone 2, and to [DVD+R], Section 13.1.3, RSV, Section 17.1, Initial Zone, and Section 18.9, Buffer Zone 2, and to [DVD+R DL], Section 13.1.3, RSV, Section 17.1, Initial Zone, and Section 18.9, Buffer Zone 2.

6.3.1 Pre-recorded DKB

A Disc manufacturer may pre-record the DKB in the Initial Zone. The format of the pre-recorded DKB is defined in Table 6-3. The Alternative Location field in the ADIP TOC entry of the corresponding DKB region shall contain the Physical Sector Number of the first sector of the structure shown in Table 6-3. This Physical Sector Number shall coincide with an ECC Block boundary.

ECC Blocks	Sectors 0..31
1	Buffer Block
K	DKB #1
1	Buffer Block
K	DKB #2
1	Buffer Block
K	DKB #3
1	Buffer Block
K	DKB #4

Table 6-3: Pre-recorded DKB

Buffer Block. All bytes in a Buffer Block shall be set to 0x00.

DKB #*n*. An EKB structure as defined in Section 5.4. The size *K* in ECC Blocks of the DKB is calculated using the equation

$$K = (N + 32767) / 32768.$$

Here *N* is the size in bytes of the DKB, as defined in Table 5-1. All bytes in DKB #*n* at byte position *N*..((*K* * 32768) – 1) shall be set to 0x00.

6.3.2 Storage of Unique ID

When writing to Buffer Zone 2, a Recorder shall randomly generate a non-zero 40-bit Unique ID to identify the Disc (see also Section 4.2). The Recorder shall store the Unique ID in the RSV field[3] of all Data Frames in Buffer Zone 2 that contain a copy of the DKB and/or padding data (i.e. the Recorder shall store the Unique ID in the headers of sectors 0x2FE10..0x2FEEF and in the headers of sectors 0x2FF10..0x2FFEF). The recorder may store the Unique ID in the RSV field of all Data Frames in Buffer Zone 2 that contain buffer block data (i.e. the Recorder may store the Unique ID in the headers of sectors 0x2FE00..0x2FE0F, in the headers of sectors 0x2FEF0..0x2FF0F, and in the headers of sectors 0x2FFF0..0x2FFFF). Table 6-4 defines the content of the RSV field.

Byte \ Bit	7	6	5	4	3	2	1	0
0	Reserved							
1	(msb)							
:	Unique ID							
5								(lsb)

Table 6-4: Unique ID

Reserved. All reserved bits shall be set to ‘0’.

Unique ID. A randomly generated 40-bit binary string that identifies the Disc.

[3] Note that this field is called CPR_MAI in [DVD-ROM].

6.3.3 Storage of DKB

When writing to Buffer Zone 2, the Recorder shall store two copies of the DKB in Buffer Zone 2 (see also Section 4.2). Table 6-5 defines the position of the two copies of the DKB in Buffer Zone 2.

Physical Sector Number	Sectors 0..31
0x2FE00 : 0x2FE0F	Buffer Block
0x2FE10 : 0x2FEEF	DKB #1
	Padding
0x2FEF0 : 0x2FEFF	Buffer Block
0x2FF00 : 0x2FF0F	Buffer Block
0x2FF10 : 0x2FFEF	DKB #2
	Padding
0x2FFF0 : 0x2FFFF	Buffer Block

Table 6-5: DKB in Buffer Zone 2

Buffer Block. All bytes in a Buffer Block shall be set to 0x00.

DKB #*n*. An EKB structure as defined in Section 5.4. The size *Q* in sectors of the DKB is calculated using the equation

$$Q = (N + 2047) / 2048.$$

Here *N* is the size in bytes of the DKB, as defined in Section 5.4. All unused bytes in DKB #*n* at byte position *N*..((Q * 2048) – 1) shall be set to 0x00.

Padding. All padding bytes shall be set to 0x00.

6.4 Data Zone

This Section 6.4 provides extensions to [DVD-Video], Section 5.2.2, Navigation Pack (NV_PCK), and Section 4.5, Data Search Information (DSI). In addition, this Section 6.4 provides extensions to [DVD+VR], Section 3.4.1, PCI_GI Extension, and to Section 4.2, VRMI General Information (VRMI_GI). Finally, this Section 6.4 provides extensions to [DVD-Video], Section 5.2.3, Video Pack (V_PCK), Section 5.2.4 Audio Pack (A_PCK), and Section 5.2.5, Sub-picture Pack (SP_PCK), and to [DVD+VR] Section 3.4.2, User Defined pack (UD_PCK), and Section 3.4.3, IEC-60958 Audio packs (IEC_PCK).

6.4.1 Navigation pack

The Navigation Packs (NV_PCK) store, amongst others, the encrypted Program Key(s) KP as well as CCI status Message Authentication Codes (MAC). Table 6-6 defines the extended NV_PCK. The NV_PCK shall be stored in an unencrypted sector.

<table>
<tr><th>Bit
Byte</th><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th><th>0</th></tr>
<tr><td>0
:
13</td><td colspan="8">Pack Header</td></tr>
<tr><td>14
:
37</td><td colspan="8">System Header</td></tr>
<tr><td>38
:
49
:
80
:
82
:
1023</td><td colspan="8">

APS

CGMS 1 | EPN 1 | PCI_PKT

CGMS 2 | EPN 2</td></tr>
<tr><td>1024
:
2014</td><td colspan="8">DSI_PKT</td></tr>
<tr><td>2015</td><td colspan="7">Reserved</td><td>New PK</td></tr>
<tr><td>2016
:
2031</td><td colspan="8">(msb)
Encrypted Program Key KP
(lsb)</td></tr>
<tr><td>2032
:
2047</td><td colspan="8">(msb)
CCI MAC
(lsb)</td></tr>
</table>

Table 6-6: Extended NV_PCK

Pack Header. See [DVD-Video], Section 5.2.1, Structure of pack.

System Header. See [DVD-Video], Section 5.2.2, Navigation Pack (NV_PCK).

PCI_PKT. See [DVD-Video], Section 4.4, Presentation Control Information (PCI), and [DVD+VR], Section 3.4.1, PCI_GI Extension.

> **APS.** Analog Protection System trigger bits. See [DVD-Video], Section 4.4.1, PCI General Information (PCI_GI).

CGMS 1/2. Copy Generation Management System control bits. See [DVD+VR], Section 3.4.1, PCI_GI Extension.

EPN 1/2. Encryption Plus Non-Assertion bit. Bit 4 of the RT_ATR_1 field defined in [DVD+VR], Section 3.4.1, PCI_GI Extension shall contain the EPN 1 bit. Bit 4 of the RT_ATR_2 field defined in [DVD+VR], Section 3.4.1, PCI_GI Extension shall contain the EPN 2 bit. The EPN 1/2 bits are valid only if the corresponding CGMS 1/2 bits are set to '00'. In that case, the EPN 1/2 bits indicate if the associated AV Sectors are encrypted as follows:

'0': The associated AV Sectors are not encrypted.
'1': The associated AV Sectors are encrypted.

DSI_PKT. See [DVD-Video], Section 4.5, Data Search Information (DSI).

Reserved. All reserved bits shall be set to '0'.

New PK. The New PK bit shall toggle with respect to the setting of the New PK bit in the preceding NV_PCK in the stream if the Encrypted Program Key KP is different from the Encrypted Program Key KP in that preceding NV_PCK.

Encrypted Program Key KP. The Encrypted Program Key KP contains the Program Key KP that is in use for all encrypted AV Sectors of the VOB.

CCI MAC. The CCI MAC shall be computed as follows:

CCI MAC = AESEncrypt(KP, CCI Digest)

Table 6-7 defines CCI Digest.

<table>
<tr><th>Bit
Byte</th><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th><th>0</th></tr>
<tr><td>0</td><td colspan="8">Digest Version</td></tr>
<tr><td>1</td><td colspan="3">APS</td><td colspan="2">CGMS 1</td><td colspan="2">CGMS 2</td><td>EPN 1</td><td>EPN 2</td></tr>
<tr><td>2</td><td colspan="8" rowspan="3">Reserved</td></tr>
<tr><td>:</td></tr>
<tr><td>11</td></tr>
<tr><td>12</td><td colspan="8" rowspan="3">(msb)
Signature
(lsb)</td></tr>
<tr><td>:</td></tr>
<tr><td>15</td></tr>
</table>

Table 6-7: CCI Digest

Digest Version. In this revision of the System Description Vidi, the value of Digest Version shall be set to 0x01.

APS. This 2-bit field shall be a copy of the APS field contained in the extended NV_PCK.

CGMS 1/2. These 2-bit fields shall be copies of the CGMS fields contained in the extended NV_PCK.

EPN 1/2. These 1-bit fields shall be copies of the EPN fields contained in the extended NV_PCK.

Reserved. All reserved bytes shall be set to 0x00.

Signature. The 4-byte signature shall have the value 0xACC1C0DE.

6.4.2 VRMI General Information

The encrypted Unique Key KU shall be stored in the general video recording manager information (VRMI_GI). Table 6-8 defines the extended VRMI_GI.

Byte \ Bit	7	6	5	4	3	2	1	0
0	VRMI_GI							
:								
80	Reserved							KU Valid
81	(msb) Encrypted Unique Key KU							
:								
96								(lsb)
:	VRMI_GI							
2047								

Table 6-8: Extended VRMI_GI

VRMI_GI. See [DVD+VR], Section 4.2, VRMI General Information.

Reserved. All reserved bits shall be set to '0'.

KU Valid. The KU Valid bit shall indicate the status of the Encrypted Unique Key as follows:

'0': The Encrypted Unique Key field does not contain valid data.
'1': The Encrypted Unique Key field contains valid data.

Encrypted Unique Key KU. The Unique Key KU, encrypted using the Disc Key KD. See also Section 4.2.

6.4.3 AV Pack

AV Sectors containing an AV Pack shall be encrypted. This is indicated in the packet header of the Video Packs, Audio Packs, Sub-Picture Packs and User Defined Packs in the Protected Video Recording. Table 6-9 defines the encrypted AV Sector.

<table>
<tr><th>Bit
Byte</th><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th><th>0</th></tr>
<tr><td>0
:
13</td><td colspan="8">Pack Header</td></tr>
<tr><td>14
:</td><td colspan="8">Packet Header</td></tr>
<tr><td>17</td><td colspan="8">Stream ID</td></tr>
<tr><td>:
20
:
127</td><td colspan="8">PES Scrambling Control
Packet Header</td></tr>
<tr><td>128
:
2047</td><td colspan="8">Encrypted AV Data</td></tr>
</table>

Table 6-9: Encrypted AV Sector

Pack Header. See [DVD-Video], Section 5.2.1, Structure of pack.

Packet Header. See [DVD-Video], Section 5.2.3, Video pack (V_PCK), Section 5.2.4, Audio pack (A_PCK), and Section 5.2.5, Sub-picture pack (SP_PCK); see [DVD+VR], Section 3.4.2, User Defined pack (UD_PCK), and Section 3.4.3, IEC-60958 Audio packs (IEC_PCK).

Stream ID. The Stream ID depends on the AV Pack type. The Stream ID in the encrypted AV Pack shall be set as defined in Table 6-10.[4] In addition to the Stream ID in the encypted AV Pack, the middle column of Table 6-10 also provides the Stream ID in the corresponding plain text AV Pack.

AV Pack type	Plain text	Encrypted
Video Pack (V_PCK)	0xE0	0xEF
Audio Pack (A_PCK)		
MPEG audio base stream	'11000*xxx*'	'11001*yyy*'
MPEG audio extension stream	'11010*xxx*'	'11011*yyy*'
All other	0xBD	0xED
Sub-picture Pack (SP_PCK)	0xBD	0xED
User Defined Pack (UD_PCK)	0xBD	0xED

Note: the three 'xxx' bits represent the audio stream number;
the three 'yyy' bits are the one's complement of the 'xxx' bits.

Table 6-10: Stream ID in plain text versus encrypted AV Packs

PES Scrambling Control. PES Scrambling Control shall be set to '11', indicating that the AV Pack contained in the AV Sector is encrypted.

(Encrypted) AV Data. The AV Pack contained in the AV Sector shall be encrypted using the Sector Key KS. See also Section 4.

[4] This avoid playback problems on video players that do not support Vidi protected recordings.

This page is intentionally left blank.

7. Drive Interface

When making and/or rendering a Protected Video Recoding, the Application (Host) shall execute all content encryption and decryption steps shown in the "Recording" and "Playback" portions of Figure 4-1. In addition, when making a Protected Video Recording the Application (Host) shall ensure that Buffer Zone 2 on the Disc contains a valid copy of the DKB (see also Section 4.2.1).
On a blank Disc, the Drive shall autonomously copy the DKB from the DKB region in the ADIP or from the Initial Zone to Buffer Zone 2 (see also Section 4.2.1). In addition, when writing the DKB in Buffer Zone 2, the Drive shall autonomously generate a non-zero Unique ID (see also Section 4.2.1).
In order to enable playback and/or recording of Protected Video Recordings, the Application (Host) shall obtain the DKB hash value and the Unique ID from the Drive using the authentication protocol that is visualized in Figure 7-1. In order to execute this authentication protocol, the Drive shall contain a unique Device ID_d, and a set of Node Keys KN_d. The Application (Host) shall contain a built-in Application Key Block AKB, and optionally a pre-computed copy of the Root Key KR_{auth} that is contained in the AKB.[5]

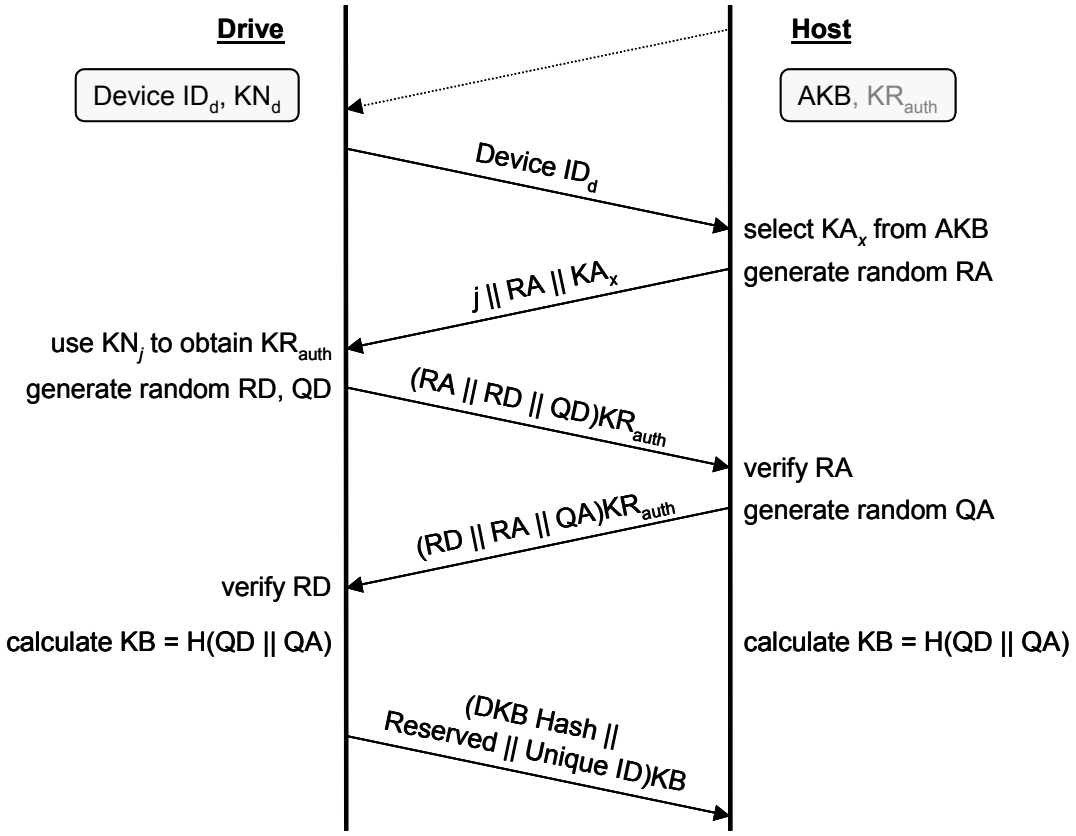

Figure 7-1: Authentication protocol

[5] The Host may also dynamically compute the Root Key KR_{auth} using the Device ID_h and the set of Node Keys KN_h (see also Section **Error! Reference source not found.**).

To successfully execute the authentication protocol, the Drive and the Application (Host) shall execute the following eight steps in the order of appearance:

Step 1. The Application (Host) shall request the Drive to return the Device ID_d.

Step 2. The Application (Host) shall use Device ID_d, to locate the Authorization Key KA_x for the Drive in the built-in AKB. If the Drive is not authorized, the Application (Host) shall abort the authentication protocol. Otherwise, the Application (Host) shall generate a 64-bit random number RA . The Application (Host) shall send the following message to the Drive:

j || RA || KA_x.

Here, j is the position of the Device ID_d bit last processed in the leaf finding algorithm defined in Section 5.2.

Step 3. The Drive shall obtain KR_{auth} as follows:

KR_{auth} = AESEncrypt(KN_j, KA_x).

Here KN_j is the key in the set of Node Keys KN_d that is associated with bit position j of Device ID_d.

Step 4. The Drive shall generate a 64-bit random number RD as well as a 128-bit random key contribution QD. The Application (Host) shall request the Drive to return the following encrypted message:

(RA || RD || QD)KR_{auth} = AESCBCEncrypt(KR_{auth}, IV2, RA || RD || QD).

The initialization vector IV2 is a 128-bit licensed constant.

Step 5. The Application (Host) shall decrypt the message received from the Drive as follows:

RA || RD || QD = AESCBCDecrypt(KR_{auth}, IV2, (RA || RD || QD)KR_{auth}).

If RA is not identical to the value that the Application (Host) has sent to the Drive in step 2, the Application (Host) shall abort the authentication protocol. Otherwise, the Application (Host) shall continue with step 6.

Step 6. The Application (Host) shall generate a 128-bit random key contribution QA. The Application (Host) shall send the following message to the Drive:

(RD || RA || QA)KR_{auth} = AESCBCDecrypt(KR_{auth}, IV2, RD || RA || QA).

The Application (Host) shall calculate the Bus Key KB as follows:

KB = AESHash(QD || QA).

Step 7. The Drive shall encrypt the message received from the Application (Host) as follows:

RD || RA || QA = AESCBCEncrypt(KR_{auth}, IV2, (RD || RA || QA)KR_{auth}).

If RD is not identical to the value that the Drive has sent to the Application (Host) in step 4, the Drive shall abort the authentication protocol. Otherwise, the Drive shall calculate the Bus Key KB as follows:

KB = AESHash(QD || QA).

Step 8. The Application (Host) shall request the Drive to return the following message:

(DKB Hash || Reserved || Unique ID)KB
= AESCBCEncrypt(KB, IV2, DKB Hash || Reserved || Unique ID).

To assemble this message, a Drive that has playback-only functionality shall set the DKB Hash field to all zeros; a Drive that has recording functionality shall read the DKB hash value from the hash region contained in the ADIP (see Section 6.2.2). The bit string Reserved consists of 88 bits that are set to '0'.

If the Drive and/or the Application (Host) have aborted the authentication protocol, a retry of the authentication protocol shall start from step 1.

Annex A Pseudo code for EKB tree tracing (informative)

The following piece of pseudo code parses the tag part of the EKB to yield the location of the Authorization Key KA_x in the key part of the EKB. Note that this pseudo code is not a straightforward implementation of the algorithm given in Section 5.2. The reason is that the EKB tree is stored in a left-to-right, top-to-bottom fashion, which renders a sequential access algorithm more efficient.
The input to this pseudo code are the Device ID, and the tags contained in the EKB (represented in Table 5-1 as Tag #1, Tag #2, …). The pseudo code reads the tag bits sequentially, starting with Tag #1. After reading a tag, the variable *Exists* contains the value of the leftmost bit of the tag, the variable *Left* contains the center bit of the tag, and the variable *Right* contains the rightmost bit of the tag.
After execution of this pseudo code, the variable *Key_Index* contains the location of the Authorization Key KA_x. *Key_Index* == 0 corresponds to Authorization Key #1. In addition, the variable *B* contains the bit position of the Device ID bit last processed. Decryption of the Authorization Key KA_x indicated by *Key_Index* using the Node Key KN_j associated with bit *B* of the Device ID yield the Root Key KR.

```
// Initialize variables
Key_Index = 0;
B = 39;
This_Level_Skip_Count = 0;
Next_Level_Skip_Count = 0;

// Process root node
Read bits of Tag #1 ( Exists, Left, Right );
Child_Exists = FALSE;
if ( Device ID bit at bit position B is a '0' ) {
        if ( Left == 0 ) Child_Exists = TRUE;
        if ( Right == 0 ) ++Next_Level_Skip_Count;
}
else { // Device ID at bit position B == 1
        if ( Left == 0 ) ++This_Level_Skip_Count;
        if ( Right == 0 ) Child_Exists = TRUE;
}

// Descend into the tree
while ( Child_Exists == TRUE ) {

        // Skip to proper child node
        while ( This_Level_Skip_Count— != 0 ) {
                Read bits of next tag ( Exists, Left, Right );
                if ( Exists == 1 ) ++Key_Index;
                if ( Left == 0 ) ++Next_Level_Skip_Count;
                if ( Right == 0 ) ++Next_Level_Skip_Count;
        }

        // Process child node
        Read bits of next tag ( Exists, Left, Right );
        Child_Exists = FALSE;
        if ( Exists == 1 ) break;
        —B;
        if ( Device ID bit at bit position B is a '0' ) {
                if ( Left == 0 ) Child_Exists = TRUE;
                This_Level_Skip_Count = Next_Level_Skip_Count;
                Next_Level_Skip_Count = 0;
                if ( Right == 0 ) ++Next_Level_Skip_Count;
        }
        else { // Device ID bit at bit position B is a '1'
                if ( Left == 0 ) ++Next_Level_Skip_Count;
                This_Level_Skip_Count = Next_Level_Skip_Count;
                Next_Level_Skip_Count = 0;
                if ( Right == 0 ) Child_Exists = TRUE;
        }

}
```

This page is intentionally left blank.

Annex B Summary of keys and constants (informative)

Table B-1 through Table B-4 summarize all cryptographic keys and constants that are used in the System Description Vidi, grouped per device type.

Name	Symbol	Size	Description
Device ID	—	40 bits	Uniquely identifies the Player or Recorder
Node Keys	KN	40 * 128 bits	Used to decrypt the Root Key KR from the DKB
Initialization Vector 1	IV1	128 bits	Used to start encryption/decryption of an AV Sector

Table B-1: Keys and constants contained in stand-alone Players and Recorders

Name	Symbol	Size	Description
Device ID	—	40 bits	Uniquely identifies a Drive
Node Keys	KN_d	40 * 128 bits	Used to decrypt the Root Key KR_{auth} from the AKB
Initialization Vector 2	IV2	128 bits	Used to start encryption/decryption of encrypted messages in the authentication protocol

Table B-2: Keys and constants contained in Drives

Name	Symbol	Size	Description
Device ID	—	40 bits	Uniquely identifies the Player or Recorder
Node Keys	KN_h	40 * 128 bits	Used to decrypt the Root Key KR from the DKB and the Root Key KR_{auth} from the AKB
Initialization Vector 1	IV1	128 bits	Used to start encryption/decryption of an AV Sector
Root Key	KR_{auth}	128 bits	Must be computed from the AKB using the Node Keys KN_h either at run-time or at compile-time (not delivered with the AKB)
Application Key Block	AKB	variable	Used to authenticate a Drive
Initialization Vector 2	IV2	128 bits	Used to start encryption/decryption of encrypted messages in the authentication protocol

Table B-3: Keys and constants contained in Applications

Name	Symbol	Size	Description
Unique ID	—	40 bits	Identifies the disc
Enabling Key Block	DKB	Variable	Contains the encrypted Root Key KR for authorized Players and Recorders
Authorization Keys	KA_x	*N* * 128 bits	The Root Key KR encrypted with a number of Node Keys KN_j; contained in the DKB
Unique Key	KU	128 bits	A key that is constant for all recordings on a Disc
Program Key	KP	128 bits	A key that is used to calculated the Sector Keys KS; it is changed for each recording and CCI change

Table B-4: Keys and constants contained on Discs

This is intentionally left blank.

Annex C EKB examples (informative)

This Annex C provides two examples of the EKB defined in Section 5. The example EKB in Section C.1 authorizes all Device IDs. The example EKB in Section C.2 revokes a few Device IDs. Section C.3 lists the Node Key sets that are used to construct the example EKBs. All Node Keys used in these example EKBs are use for illustrative purposes only and will not be present in any Player or Recorder.

C.1 Example EKB #1

Figure C-1 shows the EKB tree in the case that all Device IDs are authorized. The EKB tree consists of a root node (the black circle) and both a left-hand child node and a right-hand child node (white circles). The tags that are associated with a node are indicated by the underlined bit sequences shown to the left of each node. The Authorization Keys, indicated as KA_x, are shown to the right of the leaf nodes. The tag of the root node is '100', which indicates that the node is the root node (leftmost tag bit is '1'), and has a left-hand child node (center tag bit is '0') and a right-hand child node (rightmost tag bit is '0'). The tags of both child nodes are '111', indicating that the nodes are child nodes.

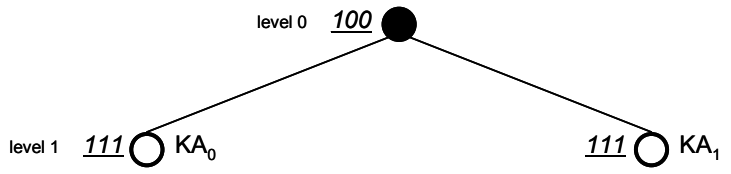

Figure C-1: EKB tree of example EKB #1

Figure C-2 shows the EKB that contains the EKB tree shown in Figure C-1. All numbers are in hexadecimal notation. The underlined parts of Figure C-2 show the EKB fields as defined in Table 5-1. The tags are obtained by concatenating all tags in a left-to right, top-to-bottom fashion, and subsequently padding to a byte boundary:

'100' || '111' || '111' || '0000000' = '1001111110000000' = 0x9F80.

The Authorization Keys KA_x are stored in a left-to-right, top-to-bottom fashion, so KA_0 comes first and KA_1 comes second. Devices 0x0000000000 through 0x7FFFFFFFFF obtain the Root Key KR by encrypting KA_0 with the Node Key KN that is associated with bit 39 of the Device ID (see Section C.3). Devices 0x8000000000 through 0xFFFFFFFFFF obtain the Root Key KR by encrypting KA_1 with the Node Key KN that is associated with bit 39 of the Device ID.
The Root Key KR of the example EKB is 0x0123456789ABCDEFFEDCBA9876543210.

```
0000:  00 00 01 44 00 00 00 01  A9 C1 01 7E 61 2F F9 7E
         EKB Size   Sequence Number      Key Check Data
0010:  9F 91 9C C3 4A 78 CD CD  E4 9F 6F 7A 55 0D 0C 39
0020:  59 E1 CA 50 …
       Authentication Data
0090:                                          … 37 5C 69 D4
00A0:  00 00 00 00 …
         Reserved
0110:                                          … 00 00 00 00
0120:  00 03 9F 80 20 95 A3 FA  63 BB 38 40 20 69 FF 5D
       Tag Count Tags                    KA0
0130:  5E 58 AD 79 34 D5 AA FC  A5 04 C3 1A 94 61 37 3A
                                          KA1
0140:  10 1D 8B EB
```

Figure C-2: Example EKB #1

C.2 Example EKB #2

Figure C-1 shows the EKB tree in the case that 6 Device IDs have been revoked. In this example the EKB tree consists of a root node (the black circle), a number of internal nodes (the gray circles) and 41 leaf nodes (the white circles). The tags that are associated with a node are indicated by the underlined bit sequences shown to the left of each node. The Authorization Keys, indicated as KA_x, are shown to the right of the leaf nodes.

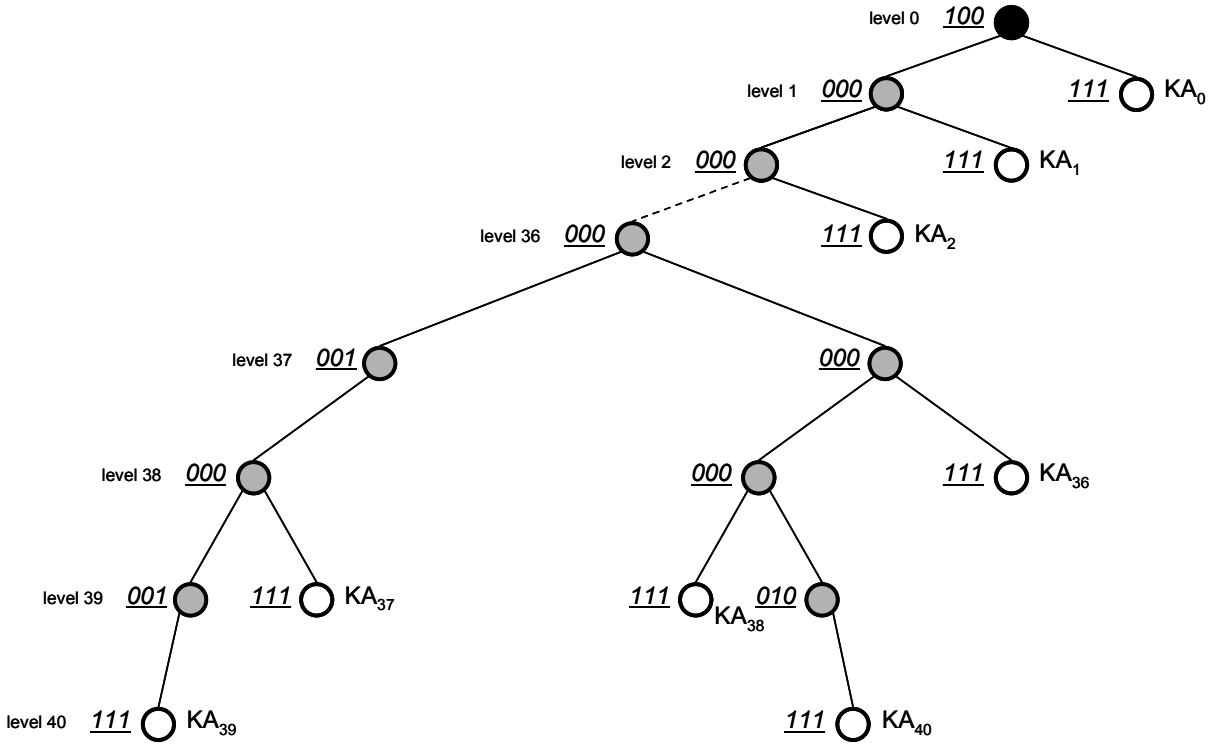

Figure C-3: EKB tree of example EKB #2

Figure C-4 shows the EKB that contains the EKB tree shown in Figure C-3. All numbers are in hexadecimal notation. The underlined parts of Figure C-4 show the EKB fields as defined in Table 5-1. The tags are obtained by concatenating all tags in a left-to right, top-to-bottom fashion, and subsequently padding to a byte boundary:

‘100’ || ‘000’ || ‘111’ || ‘000’ || ‘111’ || … || ‘111’ || ‘010’ || ‘111’ || ‘111’.

The Authorization Keys KA_x are stored in a left-to-right, top-to-bottom fashion, so KA_0 comes first, next comes KA_1, etc. Devices 0x8000000000 through 0xFFFFFFFFFF obtain the Root Key KR by encrypting KA_0 with the Node Key KN that is associated with bit 39 of the Device ID (see Section C.3). Devices 0x4000000000 through 0x7FFFFFFFFF obtain the Root Key KR by encrypting KA_1 with the Node Key KN that is associated with bit 38 of the Device ID. Devices 0x2000000000 through 0x3FFFFFFFFF obtain the Root Key KR by encrypting KA_2 with the Node Key KN that is associated with bit 37 of the Device ID. … Devices 0x000000000C through 0x000000000F obtain the Root Key KR by encrypting KA_{36} with the Node Key KN that is associated with bit 2 of the Device ID. Devices 0x0000000002 and 0x0000000003 obtain the Root Key KR by encrypting KA_{37} with the Node Key KN that is associated with bit 1 of the Device ID. Devices 0x0000000008 and 0x0000000009 obtain the Root Key KR by encrypting KA_{38} with the Node Key KN that is associated with bit 1 of the Device ID. Device 0x0000000000 obtains the Root Key KR by encrypting KA_{39} with the Node Key KN that is associated with bit 0 of the Device ID. Device 0x000000000B obtains the Root Key KR by encrypting KA_{40} with the Node Key KN that is associated with bit 0 of the Device ID.
The Root Key of the example EKB is 0xFEDCBA98765432100123456789ABCDEF.


```
0000:  00 00 03 D2 00 00 00 02  68 79 25 24 45 A8 EF 22
         EKB Size    Sequence Number      Key Check Data
0010:  56 3B 18 B7 4A B7 E7 6C  B4 EC 15 35 34 6F A9 5B
0020:  6A CA EE C5 …
       Authentication Data
0090:                                    … 89 88 B4 C0
00A0:  00 00 00 00 …
         Reserved
0110:                                    … 00 00 00 00
0120:  00 54 83 8E 38 E3 8E 38  E3 8E 38 E3 8E 38 E3 8E
       Tag Count          Tags
0130:  38 E3 8E 38 E3 8E 38 E3  8E 38 E3 8E 38 E4 01 CF
0140:  EB F0 EE 2E 76 4A A0 19  DD 60 99 90 10 9D 30 6D
                                KA0
0150:  A8 3F FE 63 38 D5 7D 15  76 FA 13 88 C8 3D EB 59
                                KA1
0160:  97 E9 E1 0C 9D 11 29 2D  03 14 5B C8 BA 6F 07 D4
                                KA2
0170:  31 DD 8F 32 CD 63 0A 0E  B8 71 40 AC A4 BA 0A 95
0180:  5F 1B AF 9A 2B A4 AE 7C  4B B0 FC A8 17 EC 89 0D
0190:  22 BE AD 98 D5 F5 4E CD  67 AF 3D AB E7 0B 80 AF
01A0:  AD 65 F9 48 99 58 1E EC  B5 06 2D 5E 46 29 C5 0B
01B0:  17 7B 6C 9E EF 10 6F 89  84 82 9E EF 86 58 D5 39
01C0:  E3 87 A6 32 93 A7 5D 64  2F 84 3B BD 5A 67 38 8F
01D0:  23 07 6F 24 72 DB 41 0E  36 87 BE 08 15 7B A0 D1
01E0:  B6 F3 A3 B9 71 C5 0E 7B  25 50 3A 20 F7 1F 41 77
01F0:  5D FD 8D 7A 48 1A 92 B0  9A BA BE 6F 23 CD 0A D6
0200:  08 BA AC 7E 1A BC FF B1  5C 89 B3 02 59 54 63 BE
0210:  65 D1 FA A1 A6 2A 06 32  01 38 8F 52 04 9F 92 3F
0220:  ED F5 D2 66 AD 5F 62 53  AC C3 5E 32 81 8F 56 B9
0230:  47 FA 99 3F 15 A4 97 E8  6E 79 B0 D0 1F B0 6D 50
0240:  CE 0E 56 40 5F E0 D2 74  8F 69 35 0C F9 49 2B 83
0250:  5D 6F CA BE 91 66 44 71  BA 99 16 A1 63 7C E4 48
0260:  25 58 15 2C 6D 83 48 5C  DE 60 12 31 FD E4 B1 CC
0270:  78 D0 47 70 72 18 AF 4C  6B 0F 8D 7D 28 78 6F 60
0280:  72 8B 45 14 46 AF F9 A6  25 50 09 BC FA 1C A8 3B
0290:  6A DC 20 48 1A E3 28 C8  91 7A E8 F8 69 55 52 53
02A0:  7B A7 E2 8F 83 0C 4F EE  60 C4 F1 12 F6 61 FA 13
02B0:  2F 20 C4 A3 90 65 70 B0  09 7D 52 6D A6 F0 F6 8F
02C0:  F5 00 6A E4 D4 B4 3D 31  0E BC 8E 51 E9 3E 56 F3
02D0:  31 30 B8 7E D2 B0 17 84  E3 D8 53 BB E7 1C 02 E1
02E0:  35 20 A0 CA 5F FD 35 C1  BF CC 81 34 22 46 84 AA
02F0:  26 53 F5 4B 59 2B 12 3D  B5 9B A6 0E F5 DB A9 88
0300:  EE 2F 10 B0 03 1E 4A 97  52 DB 7E 58 E5 4D 44 51
0310:  03 B2 99 FA 01 56 39 73  76 03 E8 99 A8 3E 3F 2E
0320:  21 1B 65 3E 2D 70 51 D3  40 EC A0 D8 1A 19 3A 07
0330:  10 7C E3 ED CE 72 93 03  6B C0 F9 11 3E A2 E0 75
0340:  73 15 B9 22 65 72 1B B5  6D D0 75 57 AD 6D 98 81
0350:  EC 01 F0 CA C6 15 85 EF  B9 FD F1 3D EB 24 DA F0
0360:  AB 94 34 3F F7 B0 DF EA  7E A3 D2 CE E2 EB FD 6E
0370:  B6 72 88 96 35 37 CA EE  8E EE 1B 1C C1 7E 88 A5
0380:  DB A1 AF 68 5D 5D 27 20  5E 44 1E 43 55 5B 9F 91
                                KA36
0390:  F0 1E A7 7C CA 22 F7 5F  00 A4 FC 2B F3 63 05 AE
                                KA37
03A0:  5B 32 9F 8D 28 DA 29 2F  FC 88 09 30 07 6A 3C E1
                                KA38
03B0:  F2 7B D5 C0 FD 61 FB 28  93 D8 92 EC 85 44 50 46
                                KA39
03C0:  89 57 A0 F4 37 EC D4 B2  2D AD EE 7D 71 C4 70 D0
                                KA40
03D0:  D2 CC
```

Figure C-4: Example EKB #2

C.3 Example Node Key sets

Figure C-5 through Figure C-20 show the sets of Node Keys KN of Devices 0x0000000000 through 0x000000000F used to create the example EKBs in this Annex C. All numbers are in hexadecimal notation. The first column shows the Device ID bit position that the Node Key KN is associated with.

```
39:  6C 4A 76 B1 C7 7C D7 25  46 43 20 8F CD D6 FF 84
38:  42 DC 8F 13 9B E0 0F 10  C1 5F 85 E8 10 D3 E2 AF
37:  C5 53 D0 E6 95 05 7A 29  0A A3 2E A4 17 21 72 DF
36:  6D E8 F3 51 55 BF 68 3B  FB A1 42 44 72 63 A2 AB
35:  D0 DD 4B 6A 65 98 67 DD  5C F0 2A 58 AE 4E B7 6E
34:  31 FD 1A 05 E1 3D C3 C5  2E 05 49 4A 08 9B 74 24
33:  1D A5 C6 84 9F 60 72 B9  63 C7 29 64 61 25 4F 9F
32:  D4 44 11 56 7B 83 DF D9  E8 32 92 7E 09 0B 06 4D
31:  71 EB FA 33 2E B1 9C A9  66 3B 62 47 4D 1C 6E FB
30:  32 28 86 71 6A 04 9E 25  E4 06 85 1A 59 BE 03 48
29:  AB 52 E3 A6 35 50 2A 5E  AF CB C3 13 13 30 3B AC
28:  5B 08 60 BD D3 1B F4 75  92 EA D3 06 41 ED D7 69
27:  65 95 50 70 2D 7E 06 E4  0A 4A 6D 63 C0 0D D1 D4
26:  5F 4B 03 F3 A9 B7 19 26  5A 8A 55 DE CD 6D D3 0D
25:  95 62 B8 B9 A2 A2 1F 97  28 81 14 F1 8A 1E 5A F2
24:  0C 7B 06 9C B5 DA 78 52  D5 46 2E CE B0 E8 79 0A
23:  76 4B 1D 41 89 3C 18 BB  1C ED E4 8A ED A2 93 E4
22:  09 5A 0E D8 6F 84 88 5C  0D A3 F2 B0 24 19 FB 98
21:  0D 55 29 0D 8A 8D 4F 0C  24 BD 44 5C D8 ED 0F E3
20:  77 CE 43 C8 C6 D5 64 AA  CD CA BA 34 A1 FD F8 04
19:  05 31 74 D0 EC 32 AF A1  C7 05 45 F4 AA 7B 4E 7C
18:  76 5C 6C 34 E8 73 82 2F  0C 72 32 20 6F 4A 3F EF
17:  AC 38 BB 62 95 BF E8 B9  61 59 C8 55 EC F7 1B E2
16:  32 B9 ED 10 EF 8F 2F A2  B0 A8 C9 65 EC C0 FB 25
15:  58 83 38 0B 9F 2B B6 85  49 B9 79 71 87 2C 68 8B
14:  0C 24 03 92 39 56 83 66  00 3D 5E 24 F3 16 D9 31
13:  E6 94 A5 5E 0C 24 CF 49  9D 0B 67 3F 7A B5 9E 9A
12:  19 34 0D AE 9A CE 97 F4  B1 39 71 27 C8 0A 5A 28
11:  4E 39 AD 97 F2 7F 0D 32  76 90 C0 40 6B 53 41 EE
10:  DC 43 32 B6 D3 AD E2 81  F7 93 76 0E AB 26 91 84
 9:  40 ED 34 B4 40 0C 39 37  B3 51 AD A4 1C A0 C1 C8
 8:  1D E1 5B 37 8D 59 EE F9  F1 72 2D 11 96 38 CE 00
 7:  40 1B E3 95 4B D7 C1 74  E4 6D DE 01 13 EC 60 38
 6:  18 4A 04 14 4E B8 F8 F8  B4 60 47 3F FF 67 E4 EF
 5:  06 3E 06 98 55 8A 68 67  77 3B BB B9 B8 42 3A AF
 4:  29 1C 00 C6 E9 CD 2E D2  66 9B BE 7D 53 BE 1D 83
 3:  98 40 28 E8 8D B0 FF 92  D7 8B E1 24 95 FD 8E 74
 2:  44 94 F2 5F 0B 2C B3 33  7A 29 3A DD 30 4A C1 8D
 1:  A3 46 4C AC 6E D7 8A CD  FE 87 C6 60 86 E1 A3 E2
 0:  69 62 F6 F9 CE 74 17 C3  3D B5 06 6D 78 E9 CE AB
```

Figure C-5: Node Key KN set of example Device ID 0x0000000000

```
39:  6C 4A 76 B1 C7 7C D7 25  46 43 20 8F CD D6 FF 84
38:  42 DC 8F 13 9B E0 0F 10  C1 5F 85 E8 10 D3 E2 AF
37:  C5 53 D0 E6 95 05 7A 29  0A A3 2E A4 17 21 72 DF
36:  6D E8 F3 51 55 BF 68 3B  FB A1 42 44 72 63 A2 AB
35:  D0 DD 4B 6A 65 98 67 DD  5C F0 2A 58 AE 4E B7 6E
34:  31 FD 1A 05 E1 3D C3 C5  2E 05 49 4A 08 9B 74 24
33:  1D A5 C6 84 9F 60 72 B9  63 C7 29 64 61 25 4F 9F
32:  D4 44 11 56 7B 83 DF D9  E8 32 92 7E 09 0B 06 4D
31:  71 EB FA 33 2E B1 9C A9  66 3B 62 47 4D 1C 6E FB
30:  32 28 86 71 6A 04 9E 25  E4 06 85 1A 59 BE 03 48
29:  AB 52 E3 A6 35 50 2A 5E  AF CB C3 13 13 30 3B AC
28:  5B 08 60 BD D3 1B F4 75  92 EA D3 06 41 ED D7 69
27:  65 95 50 70 2D 7E 06 E4  0A 4A 6D 63 C0 0D D1 D4
26:  5F 4B 03 F3 A9 B7 19 26  5A 8A 55 DE CD 6D D3 0D
25:  95 62 B8 B9 A2 A2 1F 97  28 81 14 F1 8A 1E 5A F2
24:  0C 7B 06 9C B5 DA 78 52  D5 46 2E CE B0 E8 79 0A
23:  76 4B 1D 41 89 3C 18 BB  1C ED E4 8A ED A2 93 E4
22:  09 5A 0E D8 6F 84 88 5C  0D A3 F2 B0 24 19 FB 98
21:  0D 55 29 0D 8A 8D 4F 0C  24 BD 44 5C D8 ED 0F E3
20:  77 CE 43 C8 C6 D5 64 AA  CD CA BA 34 A1 FD F8 04
19:  05 31 74 D0 EC 32 AF A1  C7 05 45 F4 AA 7B 4E 7C
18:  76 5C 6C 34 E8 73 82 2F  0C 72 32 20 6F 4A 3F EF
17:  AC 38 BB 62 95 BF E8 B9  61 59 C8 55 EC F7 1B E2
16:  32 B9 ED 10 EF 8F 2F A2  B0 A8 C9 65 EC C0 FB 25
15:  58 83 38 0B 9F 2B B6 85  49 B9 79 71 87 2C 68 8B
14:  0C 24 03 92 39 56 83 66  00 3D 5E 24 F3 16 D9 31
13:  E6 94 A5 5E 0C 24 CF 49  9D 0B 67 3F 7A B5 9E 9A
12:  19 34 0D AE 9A CE 97 F4  B1 39 71 27 C8 0A 5A 28
11:  4E 39 AD 97 F2 7F 0D 32  76 90 C0 40 6B 53 41 EE
10:  DC 43 32 B6 D3 AD E2 81  F7 93 76 0E AB 26 91 84
 9:  40 ED 34 B4 40 0C 39 37  B3 51 AD A4 1C A0 C1 C8
 8:  1D E1 5B 37 8D 59 EE F9  F1 72 2D 11 96 38 CE 00
 7:  40 1B E3 95 4B D7 C1 74  E4 6D DE 01 13 EC 60 38
 6:  18 4A 04 14 4E B8 F8 F8  B4 60 47 3F FF 67 E4 EF
 5:  06 3E 06 98 55 8A 68 67  77 3B BB B9 B8 42 3A AF
 4:  29 1C 00 C6 E9 CD 2E D2  66 9B BE 7D 53 BE 1D 83
 3:  98 40 28 E8 8D B0 FF 92  D7 8B E1 24 95 FD 8E 74
 2:  44 94 F2 5F 0B 2C B3 33  7A 29 3A DD 30 4A C1 8D
 1:  A3 46 4C AC 6E D7 8A CD  FE 87 C6 60 86 E1 A3 E2
 0:  E5 E8 F2 C1 3F F7 E9 91  F0 08 6B 31 0D 70 00 09
```

Figure C-6: Node Key KN set of example Device ID 0x0000000001

```
39:  6C 4A 76 B1 C7 7C D7 25  46 43 20 8F CD D6 FF 84
38:  42 DC 8F 13 9B E0 0F 10  C1 5F 85 E8 10 D3 E2 AF
37:  C5 53 D0 E6 95 05 7A 29  0A A3 2E A4 17 21 72 DF
36:  6D E8 F3 51 55 BF 68 3B  FB A1 42 44 72 63 A2 AB
35:  D0 DD 4B 6A 65 98 67 DD  5C F0 2A 58 AE 4E B7 6E
34:  31 FD 1A 05 E1 3D C3 C5  2E 05 49 4A 08 9B 74 24
33:  1D A5 C6 84 9F 60 72 B9  63 C7 29 64 61 25 4F 9F
32:  D4 44 11 56 7B 83 DF D9  E8 32 92 7E 09 0B 06 4D
31:  71 EB FA 33 2E B1 9C A9  66 3B 62 47 4D 1C 6E FB
30:  32 28 86 71 6A 04 9E 25  E4 06 85 1A 59 BE 03 48
29:  AB 52 E3 A6 35 50 2A 5E  AF CB C3 13 13 30 3B AC
28:  5B 08 60 BD D3 1B F4 75  92 EA D3 06 41 ED D7 69
27:  65 95 50 70 2D 7E 06 E4  0A 4A 6D 63 C0 0D D1 D4
26:  5F 4B 03 F3 A9 B7 19 26  5A 8A 55 DE CD 6D D3 0D
25:  95 62 B8 B9 A2 A2 1F 97  28 81 14 F1 8A 1E 5A F2
24:  0C 7B 06 9C B5 DA 78 52  D5 46 2E CE B0 E8 79 0A
23:  76 4B 1D 41 89 3C 18 BB  1C ED E4 8A ED A2 93 E4
22:  09 5A 0E D8 6F 84 88 5C  0D A3 F2 B0 24 19 FB 98
21:  0D 55 29 0D 8A 8D 4F 0C  24 BD 44 5C D8 ED 0F E3
20:  77 CE 43 C8 C6 D5 64 AA  CD CA BA 34 A1 FD F8 04
19:  05 31 74 D0 EC 32 AF A1  C7 05 45 F4 AA 7B 4E 7C
18:  76 5C 6C 34 E8 73 82 2F  0C 72 32 20 6F 4A 3F EF
17:  AC 38 BB 62 95 BF E8 B9  61 59 C8 55 EC F7 1B E2
16:  32 B9 ED 10 EF 8F 2F A2  B0 A8 C9 65 EC C0 FB 25
15:  58 83 38 0B 9F 2B B6 85  49 B9 79 71 87 2C 68 8B
14:  0C 24 03 92 39 56 83 66  00 3D 5E 24 F3 16 D9 31
13:  E6 94 A5 5E 0C 24 CF 49  9D 0B 67 3F 7A B5 9E 9A
12:  19 34 0D AE 9A CE 97 F4  B1 39 71 27 C8 0A 5A 28
11:  4E 39 AD 97 F2 7F 0D 32  76 90 C0 40 6B 53 41 EE
10:  DC 43 32 B6 D3 AD E2 81  F7 93 76 0E AB 26 91 84
 9:  40 ED 34 B4 40 0C 39 37  B3 51 AD A4 1C A0 C1 C8
 8:  1D E1 5B 37 8D 59 EE F9  F1 72 2D 11 96 38 CE 00
 7:  40 1B E3 95 4B D7 C1 74  E4 6D DE 01 13 EC 60 38
 6:  18 4A 04 14 4E B8 F8 F8  B4 60 47 3F FF 67 E4 EF
 5:  06 3E 06 98 55 8A 68 67  77 3B BB B9 B8 42 3A AF
 4:  29 1C 00 C6 E9 CD 2E D2  66 9B BE 7D 53 BE 1D 83
 3:  98 40 28 E8 8D B0 FF 92  D7 8B E1 24 95 FD 8E 74
 2:  44 94 F2 5F 0B 2C B3 33  7A 29 3A DD 30 4A C1 8D
 1:  13 8E CA 0F E3 70 1A 5F  E2 81 4E 03 BC 18 BC 11
 0:  A5 C3 5C 7C A8 7E 32 94  51 75 F8 1F 49 AE 79 6A
```

Figure C-7: Node Key KN set of example Device ID 0x0000000002

```
39:  6C 4A 76 B1 C7 7C D7 25  46 43 20 8F CD D6 FF 84
38:  42 DC 8F 13 9B E0 0F 10  C1 5F 85 E8 10 D3 E2 AF
37:  C5 53 D0 E6 95 05 7A 29  0A A3 2E A4 17 21 72 DF
36:  6D E8 F3 51 55 BF 68 3B  FB A1 42 44 72 63 A2 AB
35:  D0 DD 4B 6A 65 98 67 DD  5C F0 2A 58 AE 4E B7 6E
34:  31 FD 1A 05 E1 3D C3 C5  2E 05 49 4A 08 9B 74 24
33:  1D A5 C6 84 9F 60 72 B9  63 C7 29 64 61 25 4F 9F
32:  D4 44 11 56 7B 83 DF D9  E8 32 92 7E 09 0B 06 4D
31:  71 EB FA 33 2E B1 9C A9  66 3B 62 47 4D 1C 6E FB
30:  32 28 86 71 6A 04 9E 25  E4 06 85 1A 59 BE 03 48
29:  AB 52 E3 A6 35 50 2A 5E  AF CB C3 13 13 30 3B AC
28:  5B 08 60 BD D3 1B F4 75  92 EA D3 06 41 ED D7 69
27:  65 95 50 70 2D 7E 06 E4  0A 4A 6D 63 C0 0D D1 D4
26:  5F 4B 03 F3 A9 B7 19 26  5A 8A 55 DE CD 6D D3 0D
25:  95 62 B8 B9 A2 A2 1F 97  28 81 14 F1 8A 1E 5A F2
24:  0C 7B 06 9C B5 DA 78 52  D5 46 2E CE B0 E8 79 0A
23:  76 4B 1D 41 89 3C 18 BB  1C ED E4 8A ED A2 93 E4
22:  09 5A 0E D8 6F 84 88 5C  0D A3 F2 B0 24 19 FB 98
21:  0D 55 29 0D 8A 8D 4F 0C  24 BD 44 5C D8 ED 0F E3
20:  77 CE 43 C8 C6 D5 64 AA  CD CA BA 34 A1 FD F8 04
19:  05 31 74 D0 EC 32 AF A1  C7 05 45 F4 AA 7B 4E 7C
18:  76 5C 6C 34 E8 73 82 2F  0C 72 32 20 6F 4A 3F EF
17:  AC 38 BB 62 95 BF E8 B9  61 59 C8 55 EC F7 1B E2
16:  32 B9 ED 10 EF 8F 2F A2  B0 A8 C9 65 EC C0 FB 25
15:  58 83 38 0B 9F 2B B6 85  49 B9 79 71 87 2C 68 8B
14:  0C 24 03 92 39 56 83 66  00 3D 5E 24 F3 16 D9 31
13:  E6 94 A5 5E 0C 24 CF 49  9D 0B 67 3F 7A B5 9E 9A
12:  19 34 0D AE 9A CE 97 F4  B1 39 71 27 C8 0A 5A 28
11:  4E 39 AD 97 F2 7F 0D 32  76 90 C0 40 6B 53 41 EE
10:  DC 43 32 B6 D3 AD E2 81  F7 93 76 0E AB 26 91 84
 9:  40 ED 34 B4 40 0C 39 37  B3 51 AD A4 1C A0 C1 C8
 8:  1D E1 5B 37 8D 59 EE F9  F1 72 2D 11 96 38 CE 00
 7:  40 1B E3 95 4B D7 C1 74  E4 6D DE 01 13 EC 60 38
 6:  18 4A 04 14 4E B8 F8 F8  B4 60 47 3F FF 67 E4 EF
 5:  06 3E 06 98 55 8A 68 67  77 3B BB B9 B8 42 3A AF
 4:  29 1C 00 C6 E9 CD 2E D2  66 9B BE 7D 53 BE 1D 83
 3:  98 40 28 E8 8D B0 FF 92  D7 8B E1 24 95 FD 8E 74
 2:  44 94 F2 5F 0B 2C B3 33  7A 29 3A DD 30 4A C1 8D
 1:  13 8E CA 0F E3 70 1A 5F  E2 81 4E 03 BC 18 BC 11
 0:  AB E4 AC 1E 85 68 11 78  10 3A AC F0 CF 2E 89 3B
```

Figure C-8: Node Key KN set of example Device ID 0x0000000003

```
39:  6C 4A 76 B1 C7 7C D7 25  46 43 20 8F CD D6 FF 84
38:  42 DC 8F 13 9B E0 0F 10  C1 5F 85 E8 10 D3 E2 AF
37:  C5 53 D0 E6 95 05 7A 29  0A A3 2E A4 17 21 72 DF
36:  6D E8 F3 51 55 BF 68 3B  FB A1 42 44 72 63 A2 AB
35:  D0 DD 4B 6A 65 98 67 DD  5C F0 2A 58 AE 4E B7 6E
34:  31 FD 1A 05 E1 3D C3 C5  2E 05 49 4A 08 9B 74 24
33:  1D A5 C6 84 9F 60 72 B9  63 C7 29 64 61 25 4F 9F
32:  D4 44 11 56 7B 83 DF D9  E8 32 92 7E 09 0B 06 4D
31:  71 EB FA 33 2E B1 9C A9  66 3B 62 47 4D 1C 6E FB
30:  32 28 86 71 6A 04 9E 25  E4 06 85 1A 59 BE 03 48
29:  AB 52 E3 A6 35 50 2A 5E  AF CB C3 13 13 30 3B AC
28:  5B 08 60 BD D3 1B F4 75  92 EA D3 06 41 ED D7 69
27:  65 95 50 70 2D 7E 06 E4  0A 4A 6D 63 C0 0D D1 D4
26:  5F 4B 03 F3 A9 B7 19 26  5A 8A 55 DE CD 6D D3 0D
25:  95 62 B8 B9 A2 A2 1F 97  28 81 14 F1 8A 1E 5A F2
24:  0C 7B 06 9C B5 DA 78 52  D5 46 2E CE B0 E8 79 0A
23:  76 4B 1D 41 89 3C 18 BB  1C ED E4 8A ED A2 93 E4
22:  09 5A 0E D8 6F 84 88 5C  0D A3 F2 B0 24 19 FB 98
21:  0D 55 29 0D 8A 8D 4F 0C  24 BD 44 5C D8 ED 0F E3
20:  77 CE 43 C8 C6 D5 64 AA  CD CA BA 34 A1 FD F8 04
19:  05 31 74 D0 EC 32 AF A1  C7 05 45 F4 AA 7B 4E 7C
18:  76 5C 6C 34 E8 73 82 2F  0C 72 32 20 6F 4A 3F EF
17:  AC 38 BB 62 95 BF E8 B9  61 59 C8 55 EC F7 1B E2
16:  32 B9 ED 10 EF 8F 2F A2  B0 A8 C9 65 EC C0 FB 25
15:  58 83 38 0B 9F 2B B6 85  49 B9 79 71 87 2C 68 8B
14:  0C 24 03 92 39 56 83 66  00 3D 5E 24 F3 16 D9 31
13:  E6 94 A5 5E 0C 24 CF 49  9D 0B 67 3F 7A B5 9E 9A
12:  19 34 0D AE 9A CE 97 F4  B1 39 71 27 C8 0A 5A 28
11:  4E 39 AD 97 F2 7F 0D 32  76 90 C0 40 6B 53 41 EE
10:  DC 43 32 B6 D3 AD E2 81  F7 93 76 0E AB 26 91 84
 9:  40 ED 34 B4 40 0C 39 37  B3 51 AD A4 1C A0 C1 C8
 8:  1D E1 5B 37 8D 59 EE F9  F1 72 2D 11 96 38 CE 00
 7:  40 1B E3 95 4B D7 C1 74  E4 6D DE 01 13 EC 60 38
 6:  18 4A 04 14 4E B8 F8 F8  B4 60 47 3F FF 67 E4 EF
 5:  06 3E 06 98 55 8A 68 67  77 3B BB B9 B8 42 3A AF
 4:  29 1C 00 C6 E9 CD 2E D2  66 9B BE 7D 53 BE 1D 83
 3:  98 40 28 E8 8D B0 FF 92  D7 8B E1 24 95 FD 8E 74
 2:  2F 4A 96 89 38 09 D5 23  1A 2E 7E 9B 7B DB FA 9E
 1:  80 04 7F F7 9B 9B 7D 16  E2 AD 9E 7B E3 8D C5 52
 0:  01 E0 3F B3 9F 4D 34 28  34 93 4A B3 ED 44 7A 4D
```

Figure C-9: Node Key KN set of example Device ID 0x0000000004

```
39:  6C 4A 76 B1 C7 7C D7 25  46 43 20 8F CD D6 FF 84
38:  42 DC 8F 13 9B E0 0F 10  C1 5F 85 E8 10 D3 E2 AF
37:  C5 53 D0 E6 95 05 7A 29  0A A3 2E A4 17 21 72 DF
36:  6D E8 F3 51 55 BF 68 3B  FB A1 42 44 72 63 A2 AB
35:  D0 DD 4B 6A 65 98 67 DD  5C F0 2A 58 AE 4E B7 6E
34:  31 FD 1A 05 E1 3D C3 C5  2E 05 49 4A 08 9B 74 24
33:  1D A5 C6 84 9F 60 72 B9  63 C7 29 64 61 25 4F 9F
32:  D4 44 11 56 7B 83 DF D9  E8 32 92 7E 09 0B 06 4D
31:  71 EB FA 33 2E B1 9C A9  66 3B 62 47 4D 1C 6E FB
30:  32 28 86 71 6A 04 9E 25  E4 06 85 1A 59 BE 03 48
29:  AB 52 E3 A6 35 50 2A 5E  AF CB C3 13 13 30 3B AC
28:  5B 08 60 BD D3 1B F4 75  92 EA D3 06 41 ED D7 69
27:  65 95 50 70 2D 7E 06 E4  0A 4A 6D 63 C0 0D D1 D4
26:  5F 4B 03 F3 A9 B7 19 26  5A 8A 55 DE CD 6D D3 0D
25:  95 62 B8 B9 A2 A2 1F 97  28 81 14 F1 8A 1E 5A F2
24:  0C 7B 06 9C B5 DA 78 52  D5 46 2E CE B0 E8 79 0A
23:  76 4B 1D 41 89 3C 18 BB  1C ED E4 8A ED A2 93 E4
22:  09 5A 0E D8 6F 84 88 5C  0D A3 F2 B0 24 19 FB 98
21:  0D 55 29 0D 8A 8D 4F 0C  24 BD 44 5C D8 ED 0F E3
20:  77 CE 43 C8 C6 D5 64 AA  CD CA BA 34 A1 FD F8 04
19:  05 31 74 D0 EC 32 AF A1  C7 05 45 F4 AA 7B 4E 7C
18:  76 5C 6C 34 E8 73 82 2F  0C 72 32 20 6F 4A 3F EF
17:  AC 38 BB 62 95 BF E8 B9  61 59 C8 55 EC F7 1B E2
16:  32 B9 ED 10 EF 8F 2F A2  B0 A8 C9 65 EC C0 FB 25
15:  58 83 38 0B 9F 2B B6 85  49 B9 79 71 87 2C 68 8B
14:  0C 24 03 92 39 56 83 66  00 3D 5E 24 F3 16 D9 31
13:  E6 94 A5 5E 0C 24 CF 49  9D 0B 67 3F 7A B5 9E 9A
12:  19 34 0D AE 9A CE 97 F4  B1 39 71 27 C8 0A 5A 28
11:  4E 39 AD 97 F2 7F 0D 32  76 90 C0 40 6B 53 41 EE
10:  DC 43 32 B6 D3 AD E2 81  F7 93 76 0E AB 26 91 84
 9:  40 ED 34 B4 40 0C 39 37  B3 51 AD A4 1C A0 C1 C8
 8:  1D E1 5B 37 8D 59 EE F9  F1 72 2D 11 96 38 CE 00
 7:  40 1B E3 95 4B D7 C1 74  E4 6D DE 01 13 EC 60 38
 6:  18 4A 04 14 4E B8 F8 F8  B4 60 47 3F FF 67 E4 EF
 5:  06 3E 06 98 55 8A 68 67  77 3B BB B9 B8 42 3A AF
 4:  29 1C 00 C6 E9 CD 2E D2  66 9B BE 7D 53 BE 1D 83
 3:  98 40 28 E8 8D B0 FF 92  D7 8B E1 24 95 FD 8E 74
 2:  2F 4A 96 89 38 09 D5 23  1A 2E 7E 9B 7B DB FA 9E
 1:  80 04 7F F7 9B 9B 7D 16  E2 AD 9E 7B E3 8D C5 52
 0:  5E 73 FA AB 81 AE FC 47  F1 CD 53 25 96 5B 55 E2
```

Figure C-10: Node Key KN set of example Device ID 0x0000000005

```
39:  6C 4A 76 B1 C7 7C D7 25  46 43 20 8F CD D6 FF 84
38:  42 DC 8F 13 9B E0 0F 10  C1 5F 85 E8 10 D3 E2 AF
37:  C5 53 D0 E6 95 05 7A 29  0A A3 2E A4 17 21 72 DF
36:  6D E8 F3 51 55 BF 68 3B  FB A1 42 44 72 63 A2 AB
35:  D0 DD 4B 6A 65 98 67 DD  5C F0 2A 58 AE 4E B7 6E
34:  31 FD 1A 05 E1 3D C3 C5  2E 05 49 4A 08 9B 74 24
33:  1D A5 C6 84 9F 60 72 B9  63 C7 29 64 61 25 4F 9F
32:  D4 44 11 56 7B 83 DF D9  E8 32 92 7E 09 0B 06 4D
31:  71 EB FA 33 2E B1 9C A9  66 3B 62 47 4D 1C 6E FB
30:  32 28 86 71 6A 04 9E 25  E4 06 85 1A 59 BE 03 48
29:  AB 52 E3 A6 35 50 2A 5E  AF CB C3 13 13 30 3B AC
28:  5B 08 60 BD D3 1B F4 75  92 EA D3 06 41 ED D7 69
27:  65 95 50 70 2D 7E 06 E4  0A 4A 6D 63 C0 0D D1 D4
26:  5F 4B 03 F3 A9 B7 19 26  5A 8A 55 DE CD 6D D3 0D
25:  95 62 B8 B9 A2 A2 1F 97  28 81 14 F1 8A 1E 5A F2
24:  0C 7B 06 9C B5 DA 78 52  D5 46 2E CE B0 E8 79 0A
23:  76 4B 1D 41 89 3C 18 BB  1C ED E4 8A ED A2 93 E4
22:  09 5A 0E D8 6F 84 88 5C  0D A3 F2 B0 24 19 FB 98
21:  0D 55 29 0D 8A 8D 4F 0C  24 BD 44 5C D8 ED 0F E3
20:  77 CE 43 C8 C6 D5 64 AA  CD CA BA 34 A1 FD F8 04
19:  05 31 74 D0 EC 32 AF A1  C7 05 45 F4 AA 7B 4E 7C
18:  76 5C 6C 34 E8 73 82 2F  0C 72 32 20 6F 4A 3F EF
17:  AC 38 BB 62 95 BF E8 B9  61 59 C8 55 EC F7 1B E2
16:  32 B9 ED 10 EF 8F 2F A2  B0 A8 C9 65 EC C0 FB 25
15:  58 83 38 0B 9F 2B B6 85  49 B9 79 71 87 2C 68 8B
14:  0C 24 03 92 39 56 83 66  00 3D 5E 24 F3 16 D9 31
13:  E6 94 A5 5E 0C 24 CF 49  9D 0B 67 3F 7A B5 9E 9A
12:  19 34 0D AE 9A CE 97 F4  B1 39 71 27 C8 0A 5A 28
11:  4E 39 AD 97 F2 7F 0D 32  76 90 C0 40 6B 53 41 EE
10:  DC 43 32 B6 D3 AD E2 81  F7 93 76 0E AB 26 91 84
 9:  40 ED 34 B4 40 0C 39 37  B3 51 AD A4 1C A0 C1 C8
 8:  1D E1 5B 37 8D 59 EE F9  F1 72 2D 11 96 38 CE 00
 7:  40 1B E3 95 4B D7 C1 74  E4 6D DE 01 13 EC 60 38
 6:  18 4A 04 14 4E B8 F8 F8  B4 60 47 3F FF 67 E4 EF
 5:  06 3E 06 98 55 8A 68 67  77 3B BB B9 B8 42 3A AF
 4:  29 1C 00 C6 E9 CD 2E D2  66 9B BE 7D 53 BE 1D 83
 3:  98 40 28 E8 8D B0 FF 92  D7 8B E1 24 95 FD 8E 74
 2:  2F 4A 96 89 38 09 D5 23  1A 2E 7E 9B 7B DB FA 9E
 1:  8A 17 84 BE 07 80 F0 65  F1 8B F8 34 36 78 AE D3
 0:  91 CB 41 35 3E E8 C8 C9  00 61 86 4C DB 3C 67 99
```

Figure C-11: Node Key KN set of example Device ID 0x0000000006

```
39:  6C 4A 76 B1 C7 7C D7 25  46 43 20 8F CD D6 FF 84
38:  42 DC 8F 13 9B E0 0F 10  C1 5F 85 E8 10 D3 E2 AF
37:  C5 53 D0 E6 95 05 7A 29  0A A3 2E A4 17 21 72 DF
36:  6D E8 F3 51 55 BF 68 3B  FB A1 42 44 72 63 A2 AB
35:  D0 DD 4B 6A 65 98 67 DD  5C F0 2A 58 AE 4E B7 6E
34:  31 FD 1A 05 E1 3D C3 C5  2E 05 49 4A 08 9B 74 24
33:  1D A5 C6 84 9F 60 72 B9  63 C7 29 64 61 25 4F 9F
32:  D4 44 11 56 7B 83 DF D9  E8 32 92 7E 09 0B 06 4D
31:  71 EB FA 33 2E B1 9C A9  66 3B 62 47 4D 1C 6E FB
30:  32 28 86 71 6A 04 9E 25  E4 06 85 1A 59 BE 03 48
29:  AB 52 E3 A6 35 50 2A 5E  AF CB C3 13 13 30 3B AC
28:  5B 08 60 BD D3 1B F4 75  92 EA D3 06 41 ED D7 69
27:  65 95 50 70 2D 7E 06 E4  0A 4A 6D 63 C0 0D D1 D4
26:  5F 4B 03 F3 A9 B7 19 26  5A 8A 55 DE CD 6D D3 0D
25:  95 62 B8 B9 A2 A2 1F 97  28 81 14 F1 8A 1E 5A F2
24:  0C 7B 06 9C B5 DA 78 52  D5 46 2E CE B0 E8 79 0A
23:  76 4B 1D 41 89 3C 18 BB  1C ED E4 8A ED A2 93 E4
22:  09 5A 0E D8 6F 84 88 5C  0D A3 F2 B0 24 19 FB 98
21:  0D 55 29 0D 8A 8D 4F 0C  24 BD 44 5C D8 ED 0F E3
20:  77 CE 43 C8 C6 D5 64 AA  CD CA BA 34 A1 FD F8 04
19:  05 31 74 D0 EC 32 AF A1  C7 05 45 F4 AA 7B 4E 7C
18:  76 5C 6C 34 E8 73 82 2F  0C 72 32 20 6F 4A 3F EF
17:  AC 38 BB 62 95 BF E8 B9  61 59 C8 55 EC F7 1B E2
16:  32 B9 ED 10 EF 8F 2F A2  B0 A8 C9 65 EC C0 FB 25
15:  58 83 38 0B 9F 2B B6 85  49 B9 79 71 87 2C 68 8B
14:  0C 24 03 92 39 56 83 66  00 3D 5E 24 F3 16 D9 31
13:  E6 94 A5 5E 0C 24 CF 49  9D 0B 67 3F 7A B5 9E 9A
12:  19 34 0D AE 9A CE 97 F4  B1 39 71 27 C8 0A 5A 28
11:  4E 39 AD 97 F2 7F 0D 32  76 90 C0 40 6B 53 41 EE
10:  DC 43 32 B6 D3 AD E2 81  F7 93 76 0E AB 26 91 84
 9:  40 ED 34 B4 40 0C 39 37  B3 51 AD A4 1C A0 C1 C8
 8:  1D E1 5B 37 8D 59 EE F9  F1 72 2D 11 96 38 CE 00
 7:  40 1B E3 95 4B D7 C1 74  E4 6D DE 01 13 EC 60 38
 6:  18 4A 04 14 4E B8 F8 F8  B4 60 47 3F FF 67 E4 EF
 5:  06 3E 06 98 55 8A 68 67  77 3B BB B9 B8 42 3A AF
 4:  29 1C 00 C6 E9 CD 2E D2  66 9B BE 7D 53 BE 1D 83
 3:  98 40 28 E8 8D B0 FF 92  D7 8B E1 24 95 FD 8E 74
 2:  2F 4A 96 89 38 09 D5 23  1A 2E 7E 9B 7B DB FA 9E
 1:  8A 17 84 BE 07 80 F0 65  F1 8B F8 34 36 78 AE D3
 0:  D3 31 FF 2A 70 9A 11 95  0B 84 FA 77 63 1B F3 A6
```

Figure C-12: Node Key KN set of example Device ID 0x0000000007

```
39:  6C 4A 76 B1 C7 7C D7 25  46 43 20 8F CD D6 FF 84
38:  42 DC 8F 13 9B E0 0F 10  C1 5F 85 E8 10 D3 E2 AF
37:  C5 53 D0 E6 95 05 7A 29  0A A3 2E A4 17 21 72 DF
36:  6D E8 F3 51 55 BF 68 3B  FB A1 42 44 72 63 A2 AB
35:  D0 DD 4B 6A 65 98 67 DD  5C F0 2A 58 AE 4E B7 6E
34:  31 FD 1A 05 E1 3D C3 C5  2E 05 49 4A 08 9B 74 24
33:  1D A5 C6 84 9F 60 72 B9  63 C7 29 64 61 25 4F 9F
32:  D4 44 11 56 7B 83 DF D9  E8 32 92 7E 09 0B 06 4D
31:  71 EB FA 33 2E B1 9C A9  66 3B 62 47 4D 1C 6E FB
30:  32 28 86 71 6A 04 9E 25  E4 06 85 1A 59 BE 03 48
29:  AB 52 E3 A6 35 50 2A 5E  AF CB C3 13 13 30 3B AC
28:  5B 08 60 BD D3 1B F4 75  92 EA D3 06 41 ED D7 69
27:  65 95 50 70 2D 7E 06 E4  0A 4A 6D 63 C0 0D D1 D4
26:  5F 4B 03 F3 A9 B7 19 26  5A 8A 55 DE CD 6D D3 0D
25:  95 62 B8 B9 A2 A2 1F 97  28 81 14 F1 8A 1E 5A F2
24:  0C 7B 06 9C B5 DA 78 52  D5 46 2E CE B0 E8 79 0A
23:  76 4B 1D 41 89 3C 18 BB  1C ED E4 8A ED A2 93 E4
22:  09 5A 0E D8 6F 84 88 5C  0D A3 F2 B0 24 19 FB 98
21:  0D 55 29 0D 8A 8D 4F 0C  24 BD 44 5C D8 ED 0F E3
20:  77 CE 43 C8 C6 D5 64 AA  CD CA BA 34 A1 FD F8 04
19:  05 31 74 D0 EC 32 AF A1  C7 05 45 F4 AA 7B 4E 7C
18:  76 5C 6C 34 E8 73 82 2F  0C 72 32 20 6F 4A 3F EF
17:  AC 38 BB 62 95 BF E8 B9  61 59 C8 55 EC F7 1B E2
16:  32 B9 ED 10 EF 8F 2F A2  B0 A8 C9 65 EC C0 FB 25
15:  58 83 38 0B 9F 2B B6 85  49 B9 79 71 87 2C 68 8B
14:  0C 24 03 92 39 56 83 66  00 3D 5E 24 F3 16 D9 31
13:  E6 94 A5 5E 0C 24 CF 49  9D 0B 67 3F 7A B5 9E 9A
12:  19 34 0D AE 9A CE 97 F4  B1 39 71 27 C8 0A 5A 28
11:  4E 39 AD 97 F2 7F 0D 32  76 90 C0 40 6B 53 41 EE
10:  DC 43 32 B6 D3 AD E2 81  F7 93 76 0E AB 26 91 84
 9:  40 ED 34 B4 40 0C 39 37  B3 51 AD A4 1C A0 C1 C8
 8:  1D E1 5B 37 8D 59 EE F9  F1 72 2D 11 96 38 CE 00
 7:  40 1B E3 95 4B D7 C1 74  E4 6D DE 01 13 EC 60 38
 6:  18 4A 04 14 4E B8 F8 F8  B4 60 47 3F FF 67 E4 EF
 5:  06 3E 06 98 55 8A 68 67  77 3B BB B9 B8 42 3A AF
 4:  29 1C 00 C6 E9 CD 2E D2  66 9B BE 7D 53 BE 1D 83
 3:  CB 22 FA 13 F3 16 41 67  C3 5E D3 CA 09 AA AE C6
 2:  85 38 4B CE E2 93 A5 EC  5D D7 19 B2 7F CB 05 E3
 1:  29 69 B2 AD 97 0B EA FB  9E EA 9E C7 57 77 D2 DA
 0:  B8 AE 9E 8B E8 17 0B D6  8F 3D 4E B4 B8 3C 79 A1
```

Figure C-13: Node Key KN set of example Device ID 0x0000000008

```
39:  6C 4A 76 B1 C7 7C D7 25  46 43 20 8F CD D6 FF 84
38:  42 DC 8F 13 9B E0 0F 10  C1 5F 85 E8 10 D3 E2 AF
37:  C5 53 D0 E6 95 05 7A 29  0A A3 2E A4 17 21 72 DF
36:  6D E8 F3 51 55 BF 68 3B  FB A1 42 44 72 63 A2 AB
35:  D0 DD 4B 6A 65 98 67 DD  5C F0 2A 58 AE 4E B7 6E
34:  31 FD 1A 05 E1 3D C3 C5  2E 05 49 4A 08 9B 74 24
33:  1D A5 C6 84 9F 60 72 B9  63 C7 29 64 61 25 4F 9F
32:  D4 44 11 56 7B 83 DF D9  E8 32 92 7E 09 0B 06 4D
31:  71 EB FA 33 2E B1 9C A9  66 3B 62 47 4D 1C 6E FB
30:  32 28 86 71 6A 04 9E 25  E4 06 85 1A 59 BE 03 48
29:  AB 52 E3 A6 35 50 2A 5E  AF CB C3 13 13 30 3B AC
28:  5B 08 60 BD D3 1B F4 75  92 EA D3 06 41 ED D7 69
27:  65 95 50 70 2D 7E 06 E4  0A 4A 6D 63 C0 0D D1 D4
26:  5F 4B 03 F3 A9 B7 19 26  5A 8A 55 DE CD 6D D3 0D
25:  95 62 B8 B9 A2 A2 1F 97  28 81 14 F1 8A 1E 5A F2
24:  0C 7B 06 9C B5 DA 78 52  D5 46 2E CE B0 E8 79 0A
23:  76 4B 1D 41 89 3C 18 BB  1C ED E4 8A ED A2 93 E4
22:  09 5A 0E D8 6F 84 88 5C  0D A3 F2 B0 24 19 FB 98
21:  0D 55 29 0D 8A 8D 4F 0C  24 BD 44 5C D8 ED 0F E3
20:  77 CE 43 C8 C6 D5 64 AA  CD CA BA 34 A1 FD F8 04
19:  05 31 74 D0 EC 32 AF A1  C7 05 45 F4 AA 7B 4E 7C
18:  76 5C 6C 34 E8 73 82 2F  0C 72 32 20 6F 4A 3F EF
17:  AC 38 BB 62 95 BF E8 B9  61 59 C8 55 EC F7 1B E2
16:  32 B9 ED 10 EF 8F 2F A2  B0 A8 C9 65 EC C0 FB 25
15:  58 83 38 0B 9F 2B B6 85  49 B9 79 71 87 2C 68 8B
14:  0C 24 03 92 39 56 83 66  00 3D 5E 24 F3 16 D9 31
13:  E6 94 A5 5E 0C 24 CF 49  9D 0B 67 3F 7A B5 9E 9A
12:  19 34 0D AE 9A CE 97 F4  B1 39 71 27 C8 0A 5A 28
11:  4E 39 AD 97 F2 7F 0D 32  76 90 C0 40 6B 53 41 EE
10:  DC 43 32 B6 D3 AD E2 81  F7 93 76 0E AB 26 91 84
 9:  40 ED 34 B4 40 0C 39 37  B3 51 AD A4 1C A0 C1 C8
 8:  1D E1 5B 37 8D 59 EE F9  F1 72 2D 11 96 38 CE 00
 7:  40 1B E3 95 4B D7 C1 74  E4 6D DE 01 13 EC 60 38
 6:  18 4A 04 14 4E B8 F8 F8  B4 60 47 3F FF 67 E4 EF
 5:  06 3E 06 98 55 8A 68 67  77 3B BB B9 B8 42 3A AF
 4:  29 1C 00 C6 E9 CD 2E D2  66 9B BE 7D 53 BE 1D 83
 3:  CB 22 FA 13 F3 16 41 67  C3 5E D3 CA 09 AA AE C6
 2:  85 38 4B CE E2 93 A5 EC  5D D7 19 B2 7F CB 05 E3
 1:  29 69 B2 AD 97 0B EA FB  9E EA 9E C7 57 77 D2 DA
 0:  A2 60 C2 EC 06 29 CC 30  91 EB 2A F5 F9 5B 36 D0
```

Figure C-14: Node Key KN set of example Device ID 0x0000000009

```
39:  6C 4A 76 B1 C7 7C D7 25  46 43 20 8F CD D6 FF 84
38:  42 DC 8F 13 9B E0 0F 10  C1 5F 85 E8 10 D3 E2 AF
37:  C5 53 D0 E6 95 05 7A 29  0A A3 2E A4 17 21 72 DF
36:  6D E8 F3 51 55 BF 68 3B  FB A1 42 44 72 63 A2 AB
35:  D0 DD 4B 6A 65 98 67 DD  5C F0 2A 58 AE 4E B7 6E
34:  31 FD 1A 05 E1 3D C3 C5  2E 05 49 4A 08 9B 74 24
33:  1D A5 C6 84 9F 60 72 B9  63 C7 29 64 61 25 4F 9F
32:  D4 44 11 56 7B 83 DF D9  E8 32 92 7E 09 0B 06 4D
31:  71 EB FA 33 2E B1 9C A9  66 3B 62 47 4D 1C 6E FB
30:  32 28 86 71 6A 04 9E 25  E4 06 85 1A 59 BE 03 48
29:  AB 52 E3 A6 35 50 2A 5E  AF CB C3 13 13 30 3B AC
28:  5B 08 60 BD D3 1B F4 75  92 EA D3 06 41 ED D7 69
27:  65 95 50 70 2D 7E 06 E4  0A 4A 6D 63 C0 0D D1 D4
26:  5F 4B 03 F3 A9 B7 19 26  5A 8A 55 DE CD 6D D3 0D
25:  95 62 B8 B9 A2 A2 1F 97  28 81 14 F1 8A 1E 5A F2
24:  0C 7B 06 9C B5 DA 78 52  D5 46 2E CE B0 E8 79 0A
23:  76 4B 1D 41 89 3C 18 BB  1C ED E4 8A ED A2 93 E4
22:  09 5A 0E D8 6F 84 88 5C  0D A3 F2 B0 24 19 FB 98
21:  0D 55 29 0D 8A 8D 4F 0C  24 BD 44 5C D8 ED 0F E3
20:  77 CE 43 C8 C6 D5 64 AA  CD CA BA 34 A1 FD F8 04
19:  05 31 74 D0 EC 32 AF A1  C7 05 45 F4 AA 7B 4E 7C
18:  76 5C 6C 34 E8 73 82 2F  0C 72 32 20 6F 4A 3F EF
17:  AC 38 BB 62 95 BF E8 B9  61 59 C8 55 EC F7 1B E2
16:  32 B9 ED 10 EF 8F 2F A2  B0 A8 C9 65 EC C0 FB 25
15:  58 83 38 0B 9F 2B B6 85  49 B9 79 71 87 2C 68 8B
14:  0C 24 03 92 39 56 83 66  00 3D 5E 24 F3 16 D9 31
13:  E6 94 A5 5E 0C 24 CF 49  9D 0B 67 3F 7A B5 9E 9A
12:  19 34 0D AE 9A CE 97 F4  B1 39 71 27 C8 0A 5A 28
11:  4E 39 AD 97 F2 7F 0D 32  76 90 C0 40 6B 53 41 EE
10:  DC 43 32 B6 D3 AD E2 81  F7 93 76 0E AB 26 91 84
 9:  40 ED 34 B4 40 0C 39 37  B3 51 AD A4 1C A0 C1 C8
 8:  1D E1 5B 37 8D 59 EE F9  F1 72 2D 11 96 38 CE 00
 7:  40 1B E3 95 4B D7 C1 74  E4 6D DE 01 13 EC 60 38
 6:  18 4A 04 14 4E B8 F8 F8  B4 60 47 3F FF 67 E4 EF
 5:  06 3E 06 98 55 8A 68 67  77 3B BB B9 B8 42 3A AF
 4:  29 1C 00 C6 E9 CD 2E D2  66 9B BE 7D 53 BE 1D 83
 3:  CB 22 FA 13 F3 16 41 67  C3 5E D3 CA 09 AA AE C6
 2:  85 38 4B CE E2 93 A5 EC  5D D7 19 B2 7F CB 05 E3
 1:  E4 DA 9A A4 A8 78 5A 63  E8 5C 39 B4 0D 8A E8 EC
 0:  9C E4 69 8C AF A3 2D E8  4E 5D 41 9D FE B5 CC B4
```

Figure C-15: Node Key KN set of example Device ID 0x000000000A

```
39:  6C 4A 76 B1 C7 7C D7 25  46 43 20 8F CD D6 FF 84
38:  42 DC 8F 13 9B E0 0F 10  C1 5F 85 E8 10 D3 E2 AF
37:  C5 53 D0 E6 95 05 7A 29  0A A3 2E A4 17 21 72 DF
36:  6D E8 F3 51 55 BF 68 3B  FB A1 42 44 72 63 A2 AB
35:  D0 DD 4B 6A 65 98 67 DD  5C F0 2A 58 AE 4E B7 6E
34:  31 FD 1A 05 E1 3D C3 C5  2E 05 49 4A 08 9B 74 24
33:  1D A5 C6 84 9F 60 72 B9  63 C7 29 64 61 25 4F 9F
32:  D4 44 11 56 7B 83 DF D9  E8 32 92 7E 09 0B 06 4D
31:  71 EB FA 33 2E B1 9C A9  66 3B 62 47 4D 1C 6E FB
30:  32 28 86 71 6A 04 9E 25  E4 06 85 1A 59 BE 03 48
29:  AB 52 E3 A6 35 50 2A 5E  AF CB C3 13 13 30 3B AC
28:  5B 08 60 BD D3 1B F4 75  92 EA D3 06 41 ED D7 69
27:  65 95 50 70 2D 7E 06 E4  0A 4A 6D 63 C0 0D D1 D4
26:  5F 4B 03 F3 A9 B7 19 26  5A 8A 55 DE CD 6D D3 0D
25:  95 62 B8 B9 A2 A2 1F 97  28 81 14 F1 8A 1E 5A F2
24:  0C 7B 06 9C B5 DA 78 52  D5 46 2E CE B0 E8 79 0A
23:  76 4B 1D 41 89 3C 18 BB  1C ED E4 8A ED A2 93 E4
22:  09 5A 0E D8 6F 84 88 5C  0D A3 F2 B0 24 19 FB 98
21:  0D 55 29 0D 8A 8D 4F 0C  24 BD 44 5C D8 ED 0F E3
20:  77 CE 43 C8 C6 D5 64 AA  CD CA BA 34 A1 FD F8 04
19:  05 31 74 D0 EC 32 AF A1  C7 05 45 F4 AA 7B 4E 7C
18:  76 5C 6C 34 E8 73 82 2F  0C 72 32 20 6F 4A 3F EF
17:  AC 38 BB 62 95 BF E8 B9  61 59 C8 55 EC F7 1B E2
16:  32 B9 ED 10 EF 8F 2F A2  B0 A8 C9 65 EC C0 FB 25
15:  58 83 38 0B 9F 2B B6 85  49 B9 79 71 87 2C 68 8B
14:  0C 24 03 92 39 56 83 66  00 3D 5E 24 F3 16 D9 31
13:  E6 94 A5 5E 0C 24 CF 49  9D 0B 67 3F 7A B5 9E 9A
12:  19 34 0D AE 9A CE 97 F4  B1 39 71 27 C8 0A 5A 28
11:  4E 39 AD 97 F2 7F 0D 32  76 90 C0 40 6B 53 41 EE
10:  DC 43 32 B6 D3 AD E2 81  F7 93 76 0E AB 26 91 84
 9:  40 ED 34 B4 40 0C 39 37  B3 51 AD A4 1C A0 C1 C8
 8:  1D E1 5B 37 8D 59 EE F9  F1 72 2D 11 96 38 CE 00
 7:  40 1B E3 95 4B D7 C1 74  E4 6D DE 01 13 EC 60 38
 6:  18 4A 04 14 4E B8 F8 F8  B4 60 47 3F FF 67 E4 EF
 5:  06 3E 06 98 55 8A 68 67  77 3B BB B9 B8 42 3A AF
 4:  29 1C 00 C6 E9 CD 2E D2  66 9B BE 7D 53 BE 1D 83
 3:  CB 22 FA 13 F3 16 41 67  C3 5E D3 CA 09 AA AE C6
 2:  85 38 4B CE E2 93 A5 EC  5D D7 19 B2 7F CB 05 E3
 1:  E4 DA 9A A4 A8 78 5A 63  E8 5C 39 B4 0D 8A E8 EC
 0:  A7 D8 28 3A B2 C6 6E 58  B6 4D B7 45 10 CE 70 32
```

Figure C-16: Node Key KN set of example Device ID 0x000000000B

```
39:  6C 4A 76 B1 C7 7C D7 25  46 43 20 8F CD D6 FF 84
38:  42 DC 8F 13 9B E0 0F 10  C1 5F 85 E8 10 D3 E2 AF
37:  C5 53 D0 E6 95 05 7A 29  0A A3 2E A4 17 21 72 DF
36:  6D E8 F3 51 55 BF 68 3B  FB A1 42 44 72 63 A2 AB
35:  D0 DD 4B 6A 65 98 67 DD  5C F0 2A 58 AE 4E B7 6E
34:  31 FD 1A 05 E1 3D C3 C5  2E 05 49 4A 08 9B 74 24
33:  1D A5 C6 84 9F 60 72 B9  63 C7 29 64 61 25 4F 9F
32:  D4 44 11 56 7B 83 DF D9  E8 32 92 7E 09 0B 06 4D
31:  71 EB FA 33 2E B1 9C A9  66 3B 62 47 4D 1C 6E FB
30:  32 28 86 71 6A 04 9E 25  E4 06 85 1A 59 BE 03 48
29:  AB 52 E3 A6 35 50 2A 5E  AF CB C3 13 13 30 3B AC
28:  5B 08 60 BD D3 1B F4 75  92 EA D3 06 41 ED D7 69
27:  65 95 50 70 2D 7E 06 E4  0A 4A 6D 63 C0 0D D1 D4
26:  5F 4B 03 F3 A9 B7 19 26  5A 8A 55 DE CD 6D D3 0D
25:  95 62 B8 B9 A2 A2 1F 97  28 81 14 F1 8A 1E 5A F2
24:  0C 7B 06 9C B5 DA 78 52  D5 46 2E CE B0 E8 79 0A
23:  76 4B 1D 41 89 3C 18 BB  1C ED E4 8A ED A2 93 E4
22:  09 5A 0E D8 6F 84 88 5C  0D A3 F2 B0 24 19 FB 98
21:  0D 55 29 0D 8A 8D 4F 0C  24 BD 44 5C D8 ED 0F E3
20:  77 CE 43 C8 C6 D5 64 AA  CD CA BA 34 A1 FD F8 04
19:  05 31 74 D0 EC 32 AF A1  C7 05 45 F4 AA 7B 4E 7C
18:  76 5C 6C 34 E8 73 82 2F  0C 72 32 20 6F 4A 3F EF
17:  AC 38 BB 62 95 BF E8 B9  61 59 C8 55 EC F7 1B E2
16:  32 B9 ED 10 EF 8F 2F A2  B0 A8 C9 65 EC C0 FB 25
15:  58 83 38 0B 9F 2B B6 85  49 B9 79 71 87 2C 68 8B
14:  0C 24 03 92 39 56 83 66  00 3D 5E 24 F3 16 D9 31
13:  E6 94 A5 5E 0C 24 CF 49  9D 0B 67 3F 7A B5 9E 9A
12:  19 34 0D AE 9A CE 97 F4  B1 39 71 27 C8 0A 5A 28
11:  4E 39 AD 97 F2 7F 0D 32  76 90 C0 40 6B 53 41 EE
10:  DC 43 32 B6 D3 AD E2 81  F7 93 76 0E AB 26 91 84
 9:  40 ED 34 B4 40 0C 39 37  B3 51 AD A4 1C A0 C1 C8
 8:  1D E1 5B 37 8D 59 EE F9  F1 72 2D 11 96 38 CE 00
 7:  40 1B E3 95 4B D7 C1 74  E4 6D DE 01 13 EC 60 38
 6:  18 4A 04 14 4E B8 F8 F8  B4 60 47 3F FF 67 E4 EF
 5:  06 3E 06 98 55 8A 68 67  77 3B BB B9 B8 42 3A AF
 4:  29 1C 00 C6 E9 CD 2E D2  66 9B BE 7D 53 BE 1D 83
 3:  CB 22 FA 13 F3 16 41 67  C3 5E D3 CA 09 AA AE C6
 2:  40 6E A5 97 6C 21 F2 CF  F3 2F 76 95 64 5D F5 0C
 1:  08 B5 8D E9 E5 D2 10 96  8E BB E2 1B 96 69 A0 F9
 0:  9D 67 DB FD 96 98 18 E3  34 16 76 2A 8A 44 FB 97
```

Figure C-17: Node Key KN set of example Device ID 0x000000000C

```
39:  6C 4A 76 B1 C7 7C D7 25  46 43 20 8F CD D6 FF 84
38:  42 DC 8F 13 9B E0 0F 10  C1 5F 85 E8 10 D3 E2 AF
37:  C5 53 D0 E6 95 05 7A 29  0A A3 2E A4 17 21 72 DF
36:  6D E8 F3 51 55 BF 68 3B  FB A1 42 44 72 63 A2 AB
35:  D0 DD 4B 6A 65 98 67 DD  5C F0 2A 58 AE 4E B7 6E
34:  31 FD 1A 05 E1 3D C3 C5  2E 05 49 4A 08 9B 74 24
33:  1D A5 C6 84 9F 60 72 B9  63 C7 29 64 61 25 4F 9F
32:  D4 44 11 56 7B 83 DF D9  E8 32 92 7E 09 0B 06 4D
31:  71 EB FA 33 2E B1 9C A9  66 3B 62 47 4D 1C 6E FB
30:  32 28 86 71 6A 04 9E 25  E4 06 85 1A 59 BE 03 48
29:  AB 52 E3 A6 35 50 2A 5E  AF CB C3 13 13 30 3B AC
28:  5B 08 60 BD D3 1B F4 75  92 EA D3 06 41 ED D7 69
27:  65 95 50 70 2D 7E 06 E4  0A 4A 6D 63 C0 0D D1 D4
26:  5F 4B 03 F3 A9 B7 19 26  5A 8A 55 DE CD 6D D3 0D
25:  95 62 B8 B9 A2 A2 1F 97  28 81 14 F1 8A 1E 5A F2
24:  0C 7B 06 9C B5 DA 78 52  D5 46 2E CE B0 E8 79 0A
23:  76 4B 1D 41 89 3C 18 BB  1C ED E4 8A ED A2 93 E4
22:  09 5A 0E D8 6F 84 88 5C  0D A3 F2 B0 24 19 FB 98
21:  0D 55 29 0D 8A 8D 4F 0C  24 BD 44 5C D8 ED 0F E3
20:  77 CE 43 C8 C6 D5 64 AA  CD CA BA 34 A1 FD F8 04
19:  05 31 74 D0 EC 32 AF A1  C7 05 45 F4 AA 7B 4E 7C
18:  76 5C 6C 34 E8 73 82 2F  0C 72 32 20 6F 4A 3F EF
17:  AC 38 BB 62 95 BF E8 B9  61 59 C8 55 EC F7 1B E2
16:  32 B9 ED 10 EF 8F 2F A2  B0 A8 C9 65 EC C0 FB 25
15:  58 83 38 0B 9F 2B B6 85  49 B9 79 71 87 2C 68 8B
14:  0C 24 03 92 39 56 83 66  00 3D 5E 24 F3 16 D9 31
13:  E6 94 A5 5E 0C 24 CF 49  9D 0B 67 3F 7A B5 9E 9A
12:  19 34 0D AE 9A CE 97 F4  B1 39 71 27 C8 0A 5A 28
11:  4E 39 AD 97 F2 7F 0D 32  76 90 C0 40 6B 53 41 EE
10:  DC 43 32 B6 D3 AD E2 81  F7 93 76 0E AB 26 91 84
 9:  40 ED 34 B4 40 0C 39 37  B3 51 AD A4 1C A0 C1 C8
 8:  1D E1 5B 37 8D 59 EE F9  F1 72 2D 11 96 38 CE 00
 7:  40 1B E3 95 4B D7 C1 74  E4 6D DE 01 13 EC 60 38
 6:  18 4A 04 14 4E B8 F8 F8  B4 60 47 3F FF 67 E4 EF
 5:  06 3E 06 98 55 8A 68 67  77 3B BB B9 B8 42 3A AF
 4:  29 1C 00 C6 E9 CD 2E D2  66 9B BE 7D 53 BE 1D 83
 3:  CB 22 FA 13 F3 16 41 67  C3 5E D3 CA 09 AA AE C6
 2:  40 6E A5 97 6C 21 F2 CF  F3 2F 76 95 64 5D F5 0C
 1:  08 B5 8D E9 E5 D2 10 96  8E BB E2 1B 96 69 A0 F9
 0:  9D 67 DB FD 96 98 18 E3  34 16 76 2A 8A 44 FB 97
```

Figure C-18: Node Key KN set of example Device ID 0x000000000D

```
39:  6C 4A 76 B1 C7 7C D7 25  46 43 20 8F CD D6 FF 84
38:  42 DC 8F 13 9B E0 0F 10  C1 5F 85 E8 10 D3 E2 AF
37:  C5 53 D0 E6 95 05 7A 29  0A A3 2E A4 17 21 72 DF
36:  6D E8 F3 51 55 BF 68 3B  FB A1 42 44 72 63 A2 AB
35:  D0 DD 4B 6A 65 98 67 DD  5C F0 2A 58 AE 4E B7 6E
34:  31 FD 1A 05 E1 3D C3 C5  2E 05 49 4A 08 9B 74 24
33:  1D A5 C6 84 9F 60 72 B9  63 C7 29 64 61 25 4F 9F
32:  D4 44 11 56 7B 83 DF D9  E8 32 92 7E 09 0B 06 4D
31:  71 EB FA 33 2E B1 9C A9  66 3B 62 47 4D 1C 6E FB
30:  32 28 86 71 6A 04 9E 25  E4 06 85 1A 59 BE 03 48
29:  AB 52 E3 A6 35 50 2A 5E  AF CB C3 13 13 30 3B AC
28:  5B 08 60 BD D3 1B F4 75  92 EA D3 06 41 ED D7 69
27:  65 95 50 70 2D 7E 06 E4  0A 4A 6D 63 C0 0D D1 D4
26:  5F 4B 03 F3 A9 B7 19 26  5A 8A 55 DE CD 6D D3 0D
25:  95 62 B8 B9 A2 A2 1F 97  28 81 14 F1 8A 1E 5A F2
24:  0C 7B 06 9C B5 DA 78 52  D5 46 2E CE B0 E8 79 0A
23:  76 4B 1D 41 89 3C 18 BB  1C ED E4 8A ED A2 93 E4
22:  09 5A 0E D8 6F 84 88 5C  0D A3 F2 B0 24 19 FB 98
21:  0D 55 29 0D 8A 8D 4F 0C  24 BD 44 5C D8 ED 0F E3
20:  77 CE 43 C8 C6 D5 64 AA  CD CA BA 34 A1 FD F8 04
19:  05 31 74 D0 EC 32 AF A1  C7 05 45 F4 AA 7B 4E 7C
18:  76 5C 6C 34 E8 73 82 2F  0C 72 32 20 6F 4A 3F EF
17:  AC 38 BB 62 95 BF E8 B9  61 59 C8 55 EC F7 1B E2
16:  32 B9 ED 10 EF 8F 2F A2  B0 A8 C9 65 EC C0 FB 25
15:  58 83 38 0B 9F 2B B6 85  49 B9 79 71 87 2C 68 8B
14:  0C 24 03 92 39 56 83 66  00 3D 5E 24 F3 16 D9 31
13:  E6 94 A5 5E 0C 24 CF 49  9D 0B 67 3F 7A B5 9E 9A
12:  19 34 0D AE 9A CE 97 F4  B1 39 71 27 C8 0A 5A 28
11:  4E 39 AD 97 F2 7F 0D 32  76 90 C0 40 6B 53 41 EE
10:  DC 43 32 B6 D3 AD E2 81  F7 93 76 0E AB 26 91 84
 9:  40 ED 34 B4 40 0C 39 37  B3 51 AD A4 1C A0 C1 C8
 8:  1D E1 5B 37 8D 59 EE F9  F1 72 2D 11 96 38 CE 00
 7:  40 1B E3 95 4B D7 C1 74  E4 6D DE 01 13 EC 60 38
 6:  18 4A 04 14 4E B8 F8 F8  B4 60 47 3F FF 67 E4 EF
 5:  06 3E 06 98 55 8A 68 67  77 3B BB B9 B8 42 3A AF
 4:  29 1C 00 C6 E9 CD 2E D2  66 9B BE 7D 53 BE 1D 83
 3:  CB 22 FA 13 F3 16 41 67  C3 5E D3 CA 09 AA AE C6
 2:  40 6E A5 97 6C 21 F2 CF  F3 2F 76 95 64 5D F5 0C
 1:  08 B5 8D E9 E5 D2 10 96  8E BB E2 1B 96 69 A0 F9
 0:  9D 67 DB FD 96 98 18 E3  34 16 76 2A 8A 44 FB 97
```

Figure C-19: Node Key KN set of example Device ID 0x000000000E

```
39:  6C 4A 76 B1 C7 7C D7 25  46 43 20 8F CD D6 FF 84
38:  42 DC 8F 13 9B E0 0F 10  C1 5F 85 E8 10 D3 E2 AF
37:  C5 53 D0 E6 95 05 7A 29  0A A3 2E A4 17 21 72 DF
36:  6D E8 F3 51 55 BF 68 3B  FB A1 42 44 72 63 A2 AB
35:  D0 DD 4B 6A 65 98 67 DD  5C F0 2A 58 AE 4E B7 6E
34:  31 FD 1A 05 E1 3D C3 C5  2E 05 49 4A 08 9B 74 24
33:  1D A5 C6 84 9F 60 72 B9  63 C7 29 64 61 25 4F 9F
32:  D4 44 11 56 7B 83 DF D9  E8 32 92 7E 09 0B 06 4D
31:  71 EB FA 33 2E B1 9C A9  66 3B 62 47 4D 1C 6E FB
30:  32 28 86 71 6A 04 9E 25  E4 06 85 1A 59 BE 03 48
29:  AB 52 E3 A6 35 50 2A 5E  AF CB C3 13 13 30 3B AC
28:  5B 08 60 BD D3 1B F4 75  92 EA D3 06 41 ED D7 69
27:  65 95 50 70 2D 7E 06 E4  0A 4A 6D 63 C0 0D D1 D4
26:  5F 4B 03 F3 A9 B7 19 26  5A 8A 55 DE CD 6D D3 0D
25:  95 62 B8 B9 A2 A2 1F 97  28 81 14 F1 8A 1E 5A F2
24:  0C 7B 06 9C B5 DA 78 52  D5 46 2E CE B0 E8 79 0A
23:  76 4B 1D 41 89 3C 18 BB  1C ED E4 8A ED A2 93 E4
22:  09 5A 0E D8 6F 84 88 5C  0D A3 F2 B0 24 19 FB 98
21:  0D 55 29 0D 8A 8D 4F 0C  24 BD 44 5C D8 ED 0F E3
20:  77 CE 43 C8 C6 D5 64 AA  CD CA BA 34 A1 FD F8 04
19:  05 31 74 D0 EC 32 AF A1  C7 05 45 F4 AA 7B 4E 7C
18:  76 5C 6C 34 E8 73 82 2F  0C 72 32 20 6F 4A 3F EF
17:  AC 38 BB 62 95 BF E8 B9  61 59 C8 55 EC F7 1B E2
16:  32 B9 ED 10 EF 8F 2F A2  B0 A8 C9 65 EC C0 FB 25
15:  58 83 38 0B 9F 2B B6 85  49 B9 79 71 87 2C 68 8B
14:  0C 24 03 92 39 56 83 66  00 3D 5E 24 F3 16 D9 31
13:  E6 94 A5 5E 0C 24 CF 49  9D 0B 67 3F 7A B5 9E 9A
12:  19 34 0D AE 9A CE 97 F4  B1 39 71 27 C8 0A 5A 28
11:  4E 39 AD 97 F2 7F 0D 32  76 90 C0 40 6B 53 41 EE
10:  DC 43 32 B6 D3 AD E2 81  F7 93 76 0E AB 26 91 84
 9:  40 ED 34 B4 40 0C 39 37  B3 51 AD A4 1C A0 C1 C8
 8:  1D E1 5B 37 8D 59 EE F9  F1 72 2D 11 96 38 CE 00
 7:  40 1B E3 95 4B D7 C1 74  E4 6D DE 01 13 EC 60 38
 6:  18 4A 04 14 4E B8 F8 F8  B4 60 47 3F FF 67 E4 EF
 5:  06 3E 06 98 55 8A 68 67  77 3B BB B9 B8 42 3A AF
 4:  29 1C 00 C6 E9 CD 2E D2  66 9B BE 7D 53 BE 1D 83
 3:  CB 22 FA 13 F3 16 41 67  C3 5E D3 CA 09 AA AE C6
 2:  40 6E A5 97 6C 21 F2 CF  F3 2F 76 95 64 5D F5 0C
 1:  08 B5 8D E9 E5 D2 10 96  8E BB E2 1B 96 69 A0 F9
 0:  9D 67 DB FD 96 98 18 E3  34 16 76 2A 8A 44 FB 97
```

Figure C-20: Node Key KN set of example Device ID 0x000000000F

Figure C-21 shows the relevant Node Keys KN of Devices 0x0000000010 through 0xFFFFFFFFFF used to create the example EKBs in Section C.1 and Section C.2. All numbers are in hexadecimal notation. The first column shows a Device ID range; the second column shows the Device ID bit position that is relevant for the Device ID range; the third column shows the Node Key KN that is associated with the relevant bit position.

Device ID range	Bit Position	Associated Node Key
8000000000…FFFFFFFFFF	39	0E 9D 39 D2 38 2A 81 E6 B9 06 C6 44 59 50 1A C0
4000000000…7FFFFFFFFF	38	84 A2 87 F1 6C 73 05 01 FE DF 4A D0 71 D6 5A 55
2000000000…3FFFFFFFFF	37	3F BA DB C1 D0 11 D6 0F 41 B6 7C B5 D9 75 9B 3E
1000000000…1FFFFFFFFF	36	F6 4F 67 C1 1F C5 DF DD 3B 62 5D 3A 62 DD 66 81
0800000000…0FFFFFFFFF	35	93 E9 0B 34 EB A0 77 9F B4 61 CC 77 7B 05 76 D4
0400000000…07FFFFFFFF	34	D2 90 9C 11 69 DD 63 B9 B2 70 3B A7 4D AC 7A 06
0200000000…03FFFFFFFF	33	A4 B2 5A 8E AB B3 0A F1 30 26 D3 A1 32 8F A2 4F
0100000000…01FFFFFFFF	32	BB A8 0F FC E8 A1 B0 95 5A 9B 3D 00 6F E7 02 26
0080000000…00FFFFFFFF	31	E6 5F 6C FC 2C B1 C0 6B 79 5B FD 44 33 1A 69 34
0040000000…007FFFFFFF	30	1D 6D B0 B6 6E 2D 45 02 27 63 86 36 AB B5 3F 17
0020000000…003FFFFFFF	29	32 93 F5 D9 5E 76 71 F5 D5 4F 61 53 AC C2 51 54
0010000000…001FFFFFFF	28	60 F2 8A 57 E2 A2 3C 32 BB 2A CC F7 13 00 41 CC
0008000000…000FFFFFFF	27	A9 B8 BB 7F 90 5A 50 34 FC 88 16 4F 7E 51 BC 76
0004000000…0007FFFFFF	26	0F 4F B4 DD C3 DE 42 57 0A 80 39 72 74 EB E7 CD
0002000000…0003FFFFFF	25	55 0A 64 BF 24 BC B9 28 13 7C BA 76 22 2F 99 DD
0001000000…0001FFFFFF	24	46 33 D7 8E CB EF D6 DA 93 5C C3 92 D0 A7 6F 66
0000800000…0000FFFFFF	23	75 08 F0 16 0D B4 12 36 CC B8 7E 51 24 AE F7 DB
0000400000…00007FFFFF	22	92 E1 0B F6 DB 1E 73 D6 35 B4 F0 4D 83 D2 27 99
0000200000…00003FFFFF	21	B5 F1 D7 FF DA 45 D2 F9 CA 83 B0 F4 04 78 BD 82
0000100000…00001FFFFF	20	EA 06 F1 EB E0 08 FD E1 93 A6 03 50 F5 4E BC D9
0000080000…00000FFFFF	19	E7 13 18 65 87 4B AC 90 53 B6 15 4C 27 7E 83 B3
0000040000…000007FFFF	18	03 C4 B7 10 1B E5 F6 AE 54 2F 97 CD D5 B2 3A 61
0000020000…000003FFFF	17	27 16 85 4C B1 17 2D 99 37 BA DC E4 27 4B 08 27
0000010000…000001FFFF	16	46 02 99 C8 AF 0D FF 8B D4 CB 34 FC 35 DE 6D 53
0000008000…000000FFFF	15	33 41 23 3E DC CC 85 AC 45 3C 8A 3E A2 3F 9B 10
0000004000…0000007FFF	14	78 93 A8 34 A9 33 AE 07 DD 42 B1 97 89 90 34 23
0000002000…0000003FFF	13	53 11 DF 92 9F A3 81 8B 66 1C 70 B5 38 A8 90 A7
0000001000…0000001FFF	12	91 6C D9 79 25 3D DD A7 6B 31 05 42 E8 97 81 29
0000000800…0000000FFF	11	99 90 19 02 A3 C9 FE C6 32 95 5A 6A 86 D5 97 F8
0000000400…00000007FF	10	AB 59 F8 01 09 C6 26 EE 4C E1 86 BC BA C1 A0 D3
0000000200…00000003FF	9	FE 49 9E D9 3A ED 06 2F 4E F7 25 97 94 64 DA B7
0000000100…00000001FF	8	E3 14 6D B6 69 2B 3E 7C 3E C0 63 59 34 D5 9B E2
0000000080…00000000FF	7	65 E4 5A D0 BE 04 5E BF 72 C1 12 11 44 F0 20 F3
0000000040…000000007F	6	DD 99 13 A9 29 73 A5 94 CA 85 FC 65 E3 13 DE 38
0000000020…000000003F	5	33 8D CE 4B 79 ED EA 6A A3 0F 13 49 64 A4 A7 17
0000000010…000000001F	4	44 D7 36 51 5D 92 77 D1 FB ED EF 82 61 3E D2 A6

Figure C-21: Additional Node Keys KN used to construct the example EKBs

Note that none of the Node Keys KN and Root Keys KR given in this Annex C will be usable for purposes other than decoding the example EKB #1 and example EKB #2.

Annex D Summary of start-up sequence (informative)

Figure D-1 shows a summary of the actions that a Recorder must perform to start making a Protected Video Recording on a Disc. First, the Recorder must check if the disc supports Protected Video Recordings (bit 0 in byte 16 of the Physical Format Information). If that is not the case, the Recorder must notify the user that a Protected Video Recording cannot be made. Otherwise, the Recorder must check if a DKB is stored in Buffer Zone 2. If that is the case, the Recorder must check if the DKB that is stored in Buffer Zone 2 is consistent with the DKB hash value that is stored in the ADIP. If that is the case, the Recorder can retrieve the encrypted Unique Key KU from the VRMI (stored in the file VIDEO_RM.IFO) and start making the Protected Video Recording. Otherwise, the Recorder must randomly generate a new Unique Key KU, and store the new Unique Key in the VRMI. The Recorder may start making the Protected Video Recording prior to storing an encrypted copy of the Unique Key KU in the VRMI.

If the DKB is not stored in Buffer Zone 2, or if the DKB that is stored in Buffer Zone 2 is not consistent with the DKB hash value that is stored in the ADIP, the Recorder must check if the Disc is either a DVD+RW Disc, or a DVD+R Disc on which Buffer Zone 2 has not been recorded yet. If that is not the case, the Recorder must notify the user that a Protected Video Recording cannot be made. Otherwise, the Recorder must randomly generate both a new Unique Key KU and a new Unique ID, retrieve the DKB from either the ADIP or the Initial Zone, store the DKB and the Unique ID in Buffer Zone 2, and store an encrypted copy of the Unique Key KU in the VRMI. The Recorder may retrieve the DKB from the ADIP while making the Protected Video Recording.

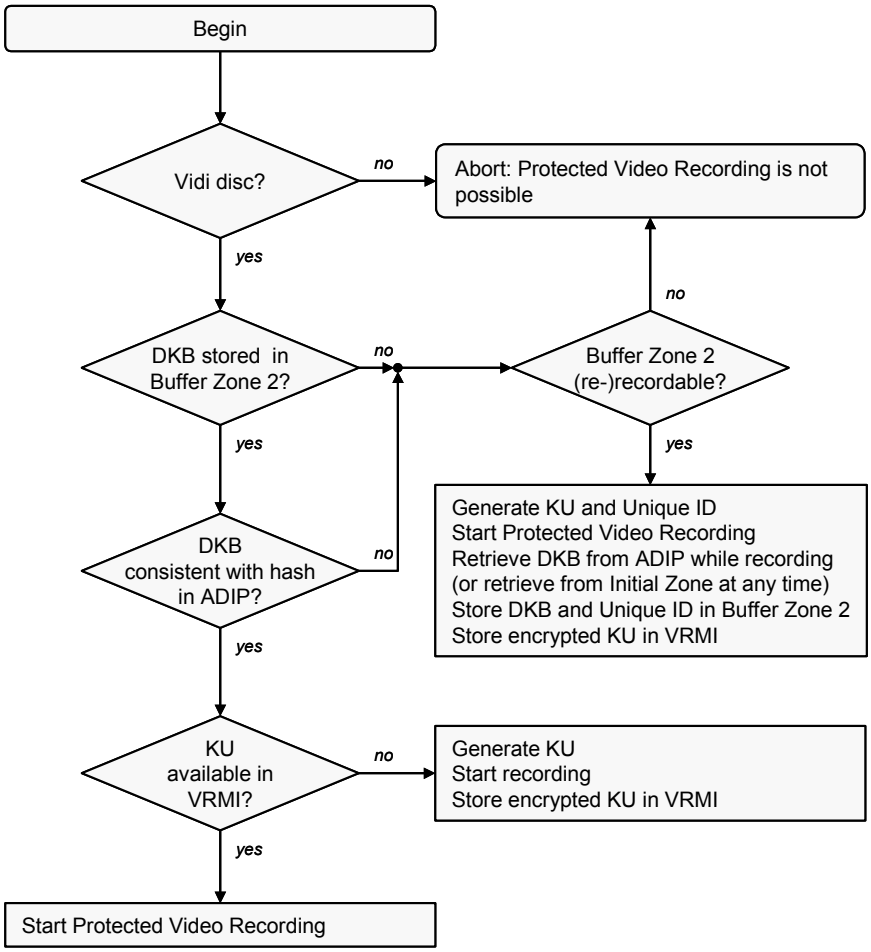

Figure D-1: Flow chart of Recorder start-up sequence

This page is intentionally left blank.

Annex E Drive Commands (informative)

This Annex E describes a command set, which a Host and a Drive can use, amongst others, to execute the authentication protocol defined in Section 7.[6] The described commands are an extension to [MMC-4]. Note that this Annex E is provided for informational purposes only. Definitive standardization of a command set that is required to implement the System Description Vidi in a Player or Recorder that consists of a Drive/Host combination will be carried out by the MMC committee.

E.1 Vidi feature

The Vidi feature specifies the capability of the Drive to process the data structures on a DVD+R/+RW disc that are specified in this System Description Vidi. The Vidi feature shall be current only if a Disc is mounted. The Vidi feature descriptor is shown in Table E-1.

Bit / Byte	7	6	5	4	3	2	1	0
0	(msb)			Feature Code				
1								(lsb)
2	Reserved			Version			Persistent	Current
3	Additional Length							
4	Reserved							
5	Reserved							
6	Reserved							
7	Reserved							

Table E-1: Vidi feature descriptor

Feature Code. The Feature Code shall be set to a value determined by the MMC committee.

Reserved. All reserved bits shall be set to ‘0’. All reserved bytes shall be set to 0x00.

Version. The version field shall be set to 0.

Persistent. The Persistent bit shall be set to ‘0’, indicating that the Vidi feature may change its current status.

Current. If the Current bit is set to ‘0’, the Vidi feature is not currently active, and certain feature dependent data may not be valid. If the Current bit is set to ‘1’, the Vidi feature is currently active and the feature dependent data is valid.

Additional Length. The Additional field shall be set to 4.

[6] A hardware Application and a Drive can also use the command set described in this Annex E. Throughout this Annex E, any reference to “Host” may be assumed to implicitly include a reference to “hardware Application.”

E.2 FORMAT UNIT command extensions

The FORMAT UNIT command formats a Disc into Host addressable logical blocks according to Host defined options. Formatting a Disc shall be performed using Format Code set to '001'. The Format Descriptor has the format defined in Table E-2.

Bit / Byte	7	6	5	4	3	2	1	0
0	(msb)							
:	Number of Blocks							
3								(lsb)
4	Format Type						Reserved	
5	(msb)							
6	Type Dependent Parameter							
7								(lsb)

Table E-2: Format Descriptor

Number of Blocks. The Number of Blocks depends on Format Type.

Format Type. Indicates the type of formatting that is requested. To request a Vidi Format, Format Type shall be set to a value determined by the MMC committee. See also Section E.2.1.

Reserved. All reserved bits shall be set to '0'.

Type Dependent Parameter. The Type Dependent Parameter depends on Format Type.

E.2.1 Vidi Format

The semantics of the Vidi Format type are as follows:

- If the mounted medium does not support Protected Video Recordings, the Drive shall terminate the command with CHECK CONDITION status. In addition, the Drive shall set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/INVALID FIELD IN PARAMETER LIST (0x05/0x26/0x00).
- Otherwise, the semantics of the Vidi Format shall be identical to the semantics of the MRW Full Format (Format Type = 0x24, see [MMC-4]), with the exception that the Drive first collects the DKB from the DKB region in the ADIP prior to (re-)starting the background formatting process, if all of the following conditions apply:
  - The Disc contains a DKB in the DKB region in the ADIP.
  - The Initial Zone does not contain a DKB.
  - Buffer Zone 2 does not contain a DKB.

E.3 REPORT KEY command extensions

The REPORT KEY command provides a general mechanism for transferring authorization information from the Drive to the Host. The Command Descriptor Block has the format defined in Table E-3.

Bit / Byte	7	6	5	4	3	2	1	0
0	Operation Code							
1	Reserved							
2	(msb)							
3								
4				Allocation Length				
5								(lsb)
6	Function Code							
7	Key Class							
8								
9				Reserved				
10								
11	Control							

Table E-3: REPORT KEY Command Descriptor Block

Operation Code. The Operation Code shall be set to 0xA4.

Reserved. All reserved bytes shall be set to 0x00.

Allocation Length. The Allocation Length specifies the maximum number of bytes that a Drive is permitted to transfer to the Host. An Allocation Length of zero indicates that no data shall be transferred. This condition shall not be considered as an error.

Function Code. The Function Code specifies the function that the Drive shall perform. The available functions are listed in Table E-4.

Function Code	Function
0x00	Reserved
0x01	DKB
0x02	Device ID
0x03	Key Contribution
0x04	DKB Hash & Unique ID
0x05	DKB Information
0x06	Reserved
:	
0xFF	

Table E-4: Functions for REPORT KEY

Key Class. The Key Class shall be set to a value determined by the MMC committee.

Control. The Control field shall have its usual meaning as specified in [MMC-4].

E.3.1 REPORT KEY DKB (Function Code 0x01)

The REPORT KEY DKB command returns the DKB that is contained in Buffer Zone 2. The semantics of the REPORT KEY DKB command are as follows (bullet items listed first take precendence over bullet items listed later):

- If the DKB is contained in Buffer Zone 2, the Drive shall return the DKB from Buffer Zone 2, and terminate with GOOD status.
- If the DKB is contained in the Initial Zone, the Drive shall write the DKB in Buffer Zone 2. If an error occurs while writing the DKB, the Drive shall terminate the command with CHECK CONDITION status. In addition, the Drive shall set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/SYSTEM RESOURCE FAILURE (0x05/0x55/0x00). Otherwise, the Drive shall return the DKB, and terminate with GOOD status.
- If the DKB is contained in the ADIP, and the Drive has completely retrieved the DKB from the DKB region in the ADIP, the Drive shall write the DKB in Buffer Zone 2. If an error occurs while writing the DKB, the Drive shall terminate the command with CHECK CONDITION status. In addition, the Drive shall set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/SYSTEM RESOURCE FAILURE (0x05/0x55/0x00). Otherwise, the Drive shall return the DKB, and terminate with GOOD status.
- Otherwise, the Drive shall terminate the command with CHECK CONDITION status. In addition the Drive shall set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/SYSTEM RESOURCE FAILURE (0x05/0x55/0x00).

The format of the returned data is defined in Table E-5.

Byte \ Bit	7	6	5	4	3	2	1	0
0	(msb)							
1	Data Length							
2								
3								(lsb)m
0	DKB							
:								
N – 1								
:	Padding							
L								

Table E-5: REPORT KEY DKB returned data format

Data Length. Data length contains the total number of bytes *L* + 4 in the returned data. The Data Length may be less than the Allocation Length in the Command Descriptor Block. This shall not be considered as an error.

DKB. An EKB structure as defined in Section 5.4.

Padding. Padding bytes may be added such that the Data Length *L* is a multiple of 4. All padding bytes shall be set to 0x00.

E.3.2 REPORT KEY Device ID (Function Code 0x02)

The REPORT KEY Device ID command returns Device ID_d of the Drive. The REPORT KEY Device ID command provides the functionality of step 1 in the authentication protocol defined in Section 7. The Drive shall return Device ID_d and terminate with GOOD status. If a previous execution of the authentication protocol is in progress, the Drive shall abort that previous execution of the authentication protocol. The format of the returned data is defined in Table E-6.

Bit / Byte	7	6	5	4	3	2	1	0
0	(msb)							
1				Data Length				
2								
3								(lsb)m
0								
:				Reserved				
30								
31	(msb)							
:				Device ID				
35								(lsb)

Table E-6: REPORT KEY Device ID returned data format

Data Length. Data length shall be set to 40.

Reserved. All reserved bytes shall be set to 0x00.

Device ID. The Device ID_d of the Drive.

E.3.3 REPORT KEY Key Contribution (Function Code 0x03)

The REPORT KEY Key Contribution command returns the key contribution QD of the Drive. The REPORT KEY Key Contribution command provides the functionality of step 4 in the authentication protocol. The semantics of the REPORT KEY Key Contribution command are as follows:

- If the authentication sequence has been violated, the Drive shall terminate the command with CHECK CONDITION status. In addition the Drive shall set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/COMMAND SEQUENCE ERROR (0x05/0x2C/0x00). A retry of the authentication protocol shall start from step 1.
- Otherwise, the Drive shall return its key contribution QD and terminate with GOOD status.

The format of the returned data is defined in Table E-7.

Bit / Byte	7	6	5	4	3	2	1	0
0	(msb)							
1	Data Length							
2								
3								(lsb)m
0	Reserved							
:								
3								
4	(msb)							
:	Encrypted Random Numbers 1							
19								(lsb)
20	(msb)							
:	Encrypted Drive Key Contribution							
35								(lsb)

Table E-7: REPORT KEY Drive Key Contribution returned data format

Data Length. Data length shall be set to 40.

Reserved. All reserved bytes shall be set to 0x00.

Encrypted Random Numbers 1. Encrypted Random Numbers 1 contains the random number RA of the Host and the random number RD of the Drive, encrypted using the Root Key KR_{auth} (see Section 7) as follows:

Encrypted Random Numbers 1 = AESEncrypt(KR_{auth}, IV2 $\oplus$ (RA || RD)).

Here IV2 is a 128-bit licensed constant.

Encrypted Drive Key Contribution. Encrypted Drive Key Contribution contains the key contribution QD of the Drive, encrypted using the Root Key KR_{auth} (see Section 7) as follows:

Encrypted Drive Key Contribution
= AESEncrypt(KR_{auth}, QD $\oplus$ Encrypted Random Numbers 1).

E.3.4 REPORT KEY DKB Hash & Unique ID (Function Code 0x04)

The REPORT KEY DKB Hash & Unique ID command returns the DKB hash value and Unique ID. The REPORT KEY DKB Hash & Unique ID command provides the functionality of step 8 in the authentication protocol. The semantics of the REPORT KEY DKB Hash & Unique ID command are as follows:

- If the authentication sequence has been violated, or if the Drive has aborted the authentication protocol in step 7, the Drive shall terminate the command with CHECK CONDITION status. In addition the Drive shall set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/COMMAND SEQUENCE ERROR (0x05/0x2C/0x00). A retry of the authentication protocol shall start from step 1.
- Otherwise, the Drive shall return the DKB Hash and Unique ID, and terminate with GOOD status.

The format of the returned data is defined in Table E-8.

Byte \ Bit	7	6	5	4	3	2	1	0
0	(msb)							
1	Data Length							
2								
3								(lsb)m
0	Reserved							
:								
3								
4	(msb)							
:	Encrypted DKB Hash							
19								(lsb)
20	(msb)							
:	Encrypted Unique ID							
35								(lsb)

Table E-8: REPORT KEY DKB Hash & Unique ID returned data format

Data Length. Data length shall be set to 40.

Reserved. All reserved bytes shall be set to 0x00.

Encrypted DKB Hash. Encrypted DKB Hash contains the DKB hash value, encrypted using the Bus Key KB as follows:

Encrypted DKB Hash = AESEncrypt(KB, IV2 ⊕ DKB Hash).

Here IV2 is a 128-bit licensed constant. A Drive that has playback-only functionality shall set DKB Hash field to all zeros, prior to encryption. A Drive that has recording functionality shall retrieve the DKB hash value from the hash region contained in the ADIP (see Section 6.2.2).

Encrypted Unique ID. Encrypted Unique ID contains the Unique ID, encrypted using the Bus Key KB as follows:

Encrypted Unique ID = AESEncrypt(KB, (Reserved || Unique ID) ⊕ Encrypted DKB Hash).

Here Reserved represents a string of 88 bits that are set to ‘0’.

E.3.5 REPORT KEY DKB Information (Function Code 0x05)

The REPORT KEY DKB command returns the information with respect to the DKB. The format of the returned data is defined in Table E-9.

Byte \ Bit	7	6	5	4	3	2	1	0
0	(msb)							
1	Data Length							
2								
3								(lsb)m
0	DKB Size							
:								
3								
4	DKB Bytes Collected							
:								
7								
8	Reserved					DKB_AD	DKB_IZ	DKB_BZ
9	Reserved							
:								
11								

Table E-9: REPORT KEY DKB returned data format

Data Length. Data length shall be set to 16.

DKB Size. The size in byte of the DKB (*N* in Table 5-1) .

DKB Bytes Collected. The number of DKB bytes that the Drive has collected so far. If the Drive has to retrieve the DKB from the DKB region in the ADIP, DKB Bytes Collected may be less than DKB Size. If the Drive has to retrieve the DKB from the Initial Zone, DKB Bytes Collected shall be equal to DKB Size. If the Drive has to retrieve the DKB from Buffer Zone 2, DKB Bytes Collected shall be equal to DKB Size.

Reserved. All reserved bits shall be set to '0'. All reserved bytes shall be set to 0x00.

DKB_AD. DKB_AD indicates if the Disc contains a DKB in the DKB region in the ADIP, as follows:

'0': The Disc does not contain a DKB in the DKB region in the ADIP.
'1': The Disc contains a DKB in the DKB region in the ADIP.

DKB_IZ. DKB_IZ indicates if the Disc contains an DKB in the Initial Zone, as follows:

'0': The Disc does not contain a DKB in the Initial Zone.
'1': The Disc contains a DKB in the Initial Zone.

DKB_BZ. DKB_BZ indicates if the Disc contains a DKB in Buffer Zone 2, as follows:

'0': The Disc does not contain a DKB in Buffer Zone 2.
'1': The Disc contains a DKB in Buffer Zone 2.

E.4 SEND KEY command extensions

The SEND KEY command provides a general mechanism for transferring authorization information from the Host to the Drive. The Command Descriptor Block has the format defined in Table E-10.

Bit / Byte	7	6	5	4	3	2	1	0
0	Operation Code							
1	Reserved							
2	(msb)							
3								
4				Parameter List Length				
5								(lsb)
6	Function Code							
7	Key Class							
8								
9				Reserved				
10								
11	Control							

Table E-10: SEND KEY Command Descriptor Block

Operation Code. The Operation Code shall be set to 0xA3.

Reserved. All reserved bytes shall be set to 0x00.

Parameter List Length. The Parameter List Length specifies the number of bytes that the Host will transfer to the Drive. A Parameter List Length of zero indicates that no data shall be transferred. This condition shall not be considered as an error.

Function Code. The Function Code specifies the function that the Drive shall perform. The available functions are listed in Table E-11.

Function Code	Function
0x00	Reserved
0x01	Authorization Key
0x02	Key Contribution
0x03	Reserved
:	
0xFF	

Table E-11: Functions for SEND KEY

Key Class. The Key Class shall be set to a value determined by the MMC committee.

Control. The Control field shall have its usual meaning as specified in [MMC-4].

E.4.1 SEND KEY Authorization Key (Function Code 0x01)

The SEND KEY Authorization Key command sends the Authorization Key KA*x* of the Drive. The SEND KEY Application Key command provides the functionality of step 2 in the authentication protocol. The semantics of the SEND KEY Authorization Key command are as follows:

- If the authentication sequence has been violated, the Drive shall terminate the command with CHECK CONDITION status. In addition the Drive shall set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/COMMAND SEQUENCE ERROR (0x05/0x2C/0x00). A retry of the authentication protocol shall start from step 1.
- Otherwise, the Drive shall accept the Authorization Key and terminate with GOOD status.

The format of the parameter data is defined in Table E-12.

Bit / Byte	7	6	5	4	3	2	1	0
0	(msb)							
1	Data Length							
2								
3								(lsb)m
0	Reserved							
:								
6								
7	Node Key Number							
8	(msb)							
:	Host Random Number							
15								(lsb)
16	(msb)							
:	Authorization Key KA_x							
31								(lsb)

Table E-12: SEND KEY Application Key parameter data

Data Length. Data length shall be set to 36.

Reserved. All reserved bytes shall be set to 0x00.

Node Key Number. Node Key Number indicates the Node Key KN_j from the set of Node Keys KN_d that the Drive shall use to obtain the Root Key KR_{auth} from the Authorization Key KA_x. For this purpose, Node Key Number contains the bit position of the Device ID_d bit that the Host has last processed in the leaf finding algorithm defined in Section 5.2.

Host Random Number. Host Random Number contains a 64-bit random number.

Authorization Key KA_x. The Authorization Key KA_x that the Host has retrieved from the Application Key Block AKB that is built-in to the Host, based on the Device ID_d the Host has obtained from the Drive.

E.4.2 SEND KEY Key Contribution (Function Code 0x02)

The SEND KEY Key Contribution command sends the Bus Key KB contribution of the Host. The SEND KEY Key Contribution command provides the functionality of steps 6 and 7 in the authentication protocol. The semantics of the SEND KEY Key Contribution command are as follows (bullet items listed first take precendence over bullet items listed later):

- If the authentication sequence has been violated, the Drive shall terminate the command with CHECK CONDITION status. In addition, the Drive shall set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/COMMAND SEQUENCE ERROR (0x05/0x2C/0x00). A retry of the authentication protocol shall start from step 1.
- If the random number RD of the Drive is not equal to the random number RD that the Drive has sent to the Host in the previous REPORT KEY Key Contribution command, the Drive shall terminate the command with CHECK CONDITION status. In addition, the Drive shall set sense bytes SK/ASC/ASCQ to ILLEGAL REQUEST/COPY PROTECTION KEY EXCHANGE FAILURE — AUTHENTICATION FAILURE (0x05/0x6F/0x00). A retry of the authentication protocol shall start from step 1.
- Otherwise, the Drive shall accept the Host Bus Key contribution and terminate with GOOD status.

The format of the parameter data is defined in Table E-13.

Bit / Byte	7	6	5	4	3	2	1	0
0	(msb)							
1	Data Length							
2								
3								(lsb)m
0	Reserved							
:								
3								
4	(msb)							
:	Encrypted Random Numbers 2							
19								(lsb)
20	(msb)							
:	Encrypted Host Key Contribution							
35								(lsb)

Table E-13: SEND KEY Host Key Contribution parameter data

Data Length. Data length shall be set to 40.

Reserved. All reserved bytes shall be set to 0x00.

Encrypted Random Numbers 2. Encrypted Random Numbers contains the random number RD of the Drive and the random number RA of the Host, encrypted using the Root Key KR_{auth} (see Section 7) as follows:

Encrypted Random Numbers 2 = AESEncrypt(KA_{auth}, IV2 ⊕ (RD || RA)).

Here IV2 is a 128-bit licensed constant.

Encrypted Host Key Contribution. Encrypted Host Key Contribution contains the key contribution QA of the Host, encrypted using the Root Key KR_{auth} (see Section 7) as follows:

Encrypted Host Key Contribution = AESEncrypt(KR_{auth}, QA ⊕ Encrypted Random Numbers 2).

E.5 Use cases

This Section E.5 provides an overview of the command sequences that a Host should issue to record or render Protected Video Recordings.

E.5.1 Authentication with a Drive

The Host should issue a REPORT KEY Device ID command to obtain Device ID_d.

The Host should retrieve the Authorization Key AK_x from the AKB built-in to the Host. In addition, the Host should generate a random number RA. The Host should issue a SEND KEY Authorization Key command to send this information to the Drive.

The Host should issue a REPORT KEY Key Contribution command to obtain the key contribution QA of the Drive. Prior to accepting the key contribution QA of the Drive, the Host should verify that the Drive has returned the correct random number RA.

The Host should issue a SEND KEY Key Contribution command to send its own key contribution QD to the Drive. With its key contribution QD, the Host should include the random number RD it has received from the Drive.

The Host should issue a REPORT KEY DKB Hash and Unique ID command to retrieve the DKB hash value and Unique ID from the Drive, which will be used to calculate the Unique Key KU for Protected Video Recordings on the Disc.

Note that the Host may execute the authentication protocol multiple times. The Drive will always accept a REPORT KEY Device ID. The Drive will interpret this command as a start of (a new execution of) the authentication protocol, i.e. the Drive will reset its internal authentication state. If another execution of the authentication protocol was in progress, that execution will be abandoned.

E.5.2 First recording on DVD+RW media

The Host should issue a GET CONFIGURATION command to check that the Drive and media support Protected Video Recordings (i.e. the Vidi feature is current).

The Host should issue a FORMAT UNIT command, requesting the Drive to format the Disc according to the Vidi format. The Drive will write the lead-in, leaving Buffer Zone 2 empty (except for the final Buffer Block, see Table 6-5). Once the initial formatting process has been completed, and the Drive has been idle for a while, and the DKB is not contained in the Initial Zone, the Drive will start collecting the DKB from the DKB region in the ADIP. If the Drive has finished collecting the DKB from the DKB region in the ADIP, or if the DKB is contained in the Initial Zone, the Drive will start the background formatting process.

The Host should authenticate with the Drive. For this purpose, the Host should issue the following sequence of commands.

The Host should authenticate with the Drive. See Section E.5.1.

If any of the command issued during authentication results in an error, the Host should retry the authentication protocol with a REPORT KEY Device ID command.

The Host should issue a REPORT KEY DKB Information command to check if the DKB is already available. If the Drive has to retrieve the DKB from the DKB region in the ADIP, the Drive returns the number of bytes of the DKB tha still has to be retrieved. This enables the Host to estimate after how much time the DKB will be available.

The Host may start recording a Protected Video Recording, while the Drive still is collecting the DKB. In the meantime, the Host may poll the Drive using a REPORT KEY DKB Information command to check on the availability of the DKB.

The Host should issue a REPORT KEY DKB command to retrieve the DKB from the Disc. This will cause the Drive to write the DKB in Buffer Zone 2. The Host should use the DKB to calculate the Disc Key KD of the Disc, and store the encrypted Unique Key KU in the VRMI.

The Host may continue or start to record a new Protected Video Recording.

E.5.3 Additional recordings

The Host should read the file system to determine that the Disc contains Protected Video Recordings.

The Host should issue a GET CONFIGURATION command to check that the Drive supports Protected Video Recordings (i.e. the Vidi feature is current).

The Host should authenticate with the Drive. See Section E.5.1.

The Host should issue a REPORT KEY DKB command to retrieve the DKB from the Disc. The Host should use the DKB to calculate the Disc Key KD of the Disc, and retrieve the encrypted Unique Key KU from the VRMI.

The Host may start to record a new Protected Video Recording

E.5.4 Playback

The Host should read the file system to determine that the Disc contains Protected Video Recordings.

The Host should issue a GET CONFIGURATION command to check that the Drive supports Protected Video Recordings (i.e. the Vidi feature is current).

The Host should authenticate with the Drive. See Section E.5.1.

The Host should issue a REPORT KEY DKB command to retrieve the DKB from the Disc. The Host should use the DKB to calculate the Disc Key KD of the Disc, and retrieve the encrypted Unique Key KU from the VRMI.

The Host may start to render a Protected Video Recording.

This page is intentionally left blank.

Annex F Extended Format Information (Informative)

The specifications in this Annex F are included by reference only, and will be included in an upcoming release of the DVD+R/+RW basic format specifications.

F.1 EFI bit

Bit 0 in byte 16 of the Physical Format Information indicates if the disc contains Extended Format Information. This bit shall be set as follows:

'0': The Data Zone ADIP of this disc does not contain Extended Format Information.
'1': The Data Zone ADIP of this disc contains Extended Format Information as defined in Section F.2.

F.2 Extended Format Information

The Extended Format Information consists of a table of contents (EFI TOC) and up to 16 distinct regions that contain additional format information. The EFI TOC defines the location and contents of the regions contained in the Extended Format Information. See Section F.2.1. The EFI TOC shall be stored in the AUX data bytes of the ADIP words in the Data Zone, starting at the ADIP word that has Physical Address 0x0C000. The regions of the Extended Format Information shall be located in the AUX data bytes of the ADIP words in the Data Zone and/or shall be present as pre-recorded areas in the main data channel. Each region contains one or more copies of a data block of a particular type, as indicated in the EFI TOC.
Figure F-1 schematically shows an example lay-out of the EFI TOC and the Vidi-defined regions that are contained in the AUX data bytes of the ADIP word in the Data Zone. The EFI TOC consists of 8 consecutive copies of an ETOC block, where each ETOC block contains the complete EFI TOC information (see Section F.2.1). The Vidi-defined hash region contains one or more copies of the DKB hash value, as specified in the EFI TOC. The Vidi-defined DKB region contains one or more copies of the DKB, as specified in the EFI TOC. Gaps may exist between any two regions. All AUX data bytes of the ADIP words in the gaps shall be set to 0x00.

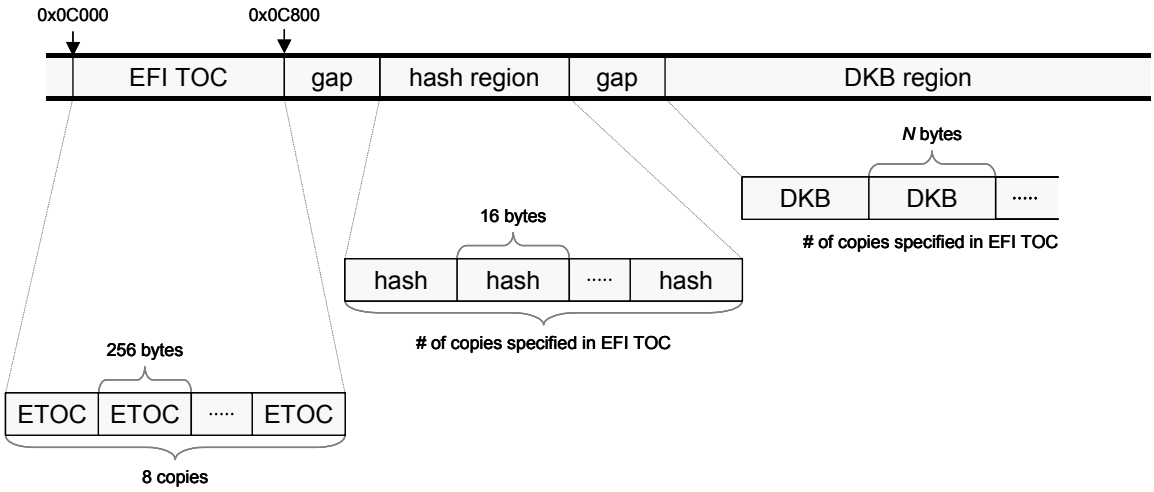

Figure F-1: Example lay-out of the Extended Format Information in the ADIP

F.2.1 EFI TOC

The EFI TOC starts at the ADIP word that has Physical Address 0x0C000. The length of the EFI TOC is 2048 consecutive ADIP words. As shown in Figure F-1, the EFI TOC consists of 8 consecutive copies of an ETOC block. The ETOC block consists of at most 16 Region Descriptors, as defined in Table F-1. The combined size of all Region Descriptors contained in the ETOC block shall be no more than 256 bytes. Unused Region Descriptors shall be set to all zeros, such that the size of the ETOC block is exactly 256 bytes.

Byte \ Bit	7	6	5	4	3	2	1	0
0	Region Descriptor #1							
:								
:	Region Descriptor #2							
:	:							
:	Region Descriptor #*n*							
255								

Table F-1: ETOC

Region Descriptor #*n*. Region Descriptor #*n* contains information with respect to the *n*-th region of the Extended Format Information ($1 \leq n \leq 16$). A Region Descriptor consists of a Basic Region Descriptor followed by zero or more Extended Region Descriptors. The format of a Basic Region Descriptor is defined in Table F-2. The format of an Extended Region Descriptor is defined in Table F-3.

Byte \ Bit	7	6	5	4	3	2	1	0
0	(msb) Region Type Identifier							
1								
2								(lsb)
3	Extent	Version Number						
4	(msb) Region Start Address							
5								(lsb)
6	(msb) Data Block Size							
:								
9								(lsb)
10	Repeat Count							
11	Reserved							Private
12	(msb) Alternative Location							
:								
15								(lsb)

Table F-2: Basic Region Descriptor

Region Type Identifier. The type of the data block that is contained in the region. Data blocks stored in different regions having the same Region Type Identifier shall be identical.

Extent. The Extent bit shall indicate if this Basic Region Descriptor is followed by an Extended Region Descriptor, as follows:

‘0’: This Basic Region Descriptor is not followed by an Extended Region Descriptor.
‘1’: This Basic Region Descriptor is followed by an Extended Region Descriptor.

Version Number. The revision of the data block type that is contained in the region.

Region Start Address. If the data block is stored in the AUX data bytes of the ADIP, the Region Start Address is given as the Physical Address of the ADIP word that contains the first byte of the data block, divided by 256. Region Start Address shall be greater than or equal to 0x00C8. If the data block is not stored in the AUX data bytes of the ADIP, the Region Start Address shall be zero. In that case the Alternative Location shall be non-zero and specify the location of the data block in the main data channel.

Data Block Size. The size in bytes of a single copy of the data block in the region.

Repeat Count. The number of consecutive copies of the data block that are contained in the region. If the data block is stored in the AUX data bytes of the ADIP and the region extends through the end of the Disc, Repeat Count shall be set to 0.

Reserved. All reserved bits shall be set to '0'.

Private. The Private bit shall indicate if a Drive is permitted to output the contents of the region, as follows:

'0': A Drive is permitted to output the contents of the region.
'1': A Drive is not permitted to output the contents of the region.

Alternative Location. In addition to, or alternative to storage in the AUX data bytes of the ADIP, the data block may be stored in a contiguous area of the main data channel. In that case, the Alternative Location specifies the location of the first Physical Sector Number in the main data channel that contains one or more copies of the data block. Otherwise, Alternative Location shall be set to zero. Note that the format of the data block as contained in the main data channel may be different from the format of the data block as contained in the AUX data bytes of the ADIP.

Bit / Byte	7	6	5	4	3	2	1	0
0	(msb)							
1	Region Type Identifier							
2								(lsb)
3	Extent	Version Number						
4	Reserved							
:								
15								

Table F-3: Extended Region Descriptor

Region Type Identifier. Region Type Identifier shall be identical to the the Region Type Identifier contained in the preceding Basic Region Descriptor.

Extent. The Extent bit shall indicate if this Extended Region Descriptor is followed by another Extended Region Descriptor, as follows:

'0': This Extended Region Descriptor is not followed by an Extended Region Descriptor.
'1': This Extended Region Descriptor is followed by an Extended Region Descriptor.

Version Number. Version Number shall be identical to the the Version Number contained in the preceding Basic Region Descriptor.

Reserved. All reserved bytes shall be set to 0x00.

This page is intentionally left blank.

Appendix B

Vidi Content Protection Agreement
Version 1.0
March 1, 2004

VIDI CONTENT PROTECTION AGREEMENT

This VIDI CONTENT PROTECTION AGREEMENT ("Agreement") by and between KONINKLIJKE PHILIPS ELECTRONICS N.V., having its registered office in Eindhoven, The Netherlands ("Philips") and
Company ("Company") identified below (Philips and Company jointly hereinafter referred to as "the Parties"), is effective as of the date executed by Parties on the signature page hereof (the "Effective Date").

Company _____

Principal Office _____

Contact Person _____

Address _____

Please place a mark in either box 1 or box 2:
1 ☐ Company enters this Agreement in the role of **Content Participant**.

2 ☐ Company enters this Agreement in the role of **Implementer** and wishes to use the Vidi technology for the following purpose(s). Please mark the applicable box(es) below:

Box	Implementer Role	Implementer Purpose	Necessary Keys
2.1 ☐	Developer	Development Only (see section 2.2 below)	none
2.2 ☐	Hardware Implementer	Development, manufacture, and/or distribution of Vidi Components, Data Drives, and products containing a Hardware Playback Function and/or Hardware Recording Function (all terms as defined below)	Hardware Device Keys, Licensed Constant 1 and Licensed Constant 2
2.3 ☐	Software Implementer	Development, manufacture, and/or distribution of Vidi Components and products containing a Software Playback Function and/or Software Recording Function (as defined below)	Software Device Keys, Licensed Constant 1, Licensed Constant 2, and Application Key Blocks
2.4 ☐	Replicator	Replication and distribution of Vidi Discs (as defined below)	none
2.5 ☐	Master Manufacturer	Manufacturing and/or distribution of masters and stampers for the manufacturing of Vidi Discs	Disc Key Blocks
2.6 ☐	Component Implementer	Development, manufacture, and/or distribution of Vidi Components that do not contain Device Keys.	Licensed Constant 1, and Licensed Constant 2

NOTE: A mark may be placed in more than one box, except that box 2.1 shall not be marked if a mark is also placed in any of boxes 2.2, 2.3, 2.4, 2.5, and 2.6.

Recitals

WHEREAS, Philips together with Hewlett-Packard Company ("HP") has developed a system for protecting certain digital audiovisual content recorded on DVD+RW and DVD+R optical digital media named "Vidi" ("Vidi," as hereinafter defined);

WHEREAS, with the aim of offering companies the convenience of entering into a single agreement under the combined Vidi Intellectual Property of both Philips and HP, HP has authorized Philips to grant non-assertion undertakings with regard to Vidi to third parties for certain content protection applications under such combined Vidi Intellectual Property and to facilitate the distribution of Keys ('Keys", as hereinafter defined);

WHEREAS, Implementer desires to obtain the right to use Vidi in Vidi Products or Vidi Components developed, manufactured and sold or otherwise distributed for use within the Field of Use (as hereinafter defined); and

WHEREAS, Philips is willing to allow Implementer the use of Vidi within the Field of Use, subject to the provisions hereof, including without limitation, strict compliance with the Compliance Rules and the Specification;

WHEREAS, Content Participant has an interest in the correct application by Implementers of Vidi in order to protect its audio-visual content that can be recorded and played back using Vidi as an encryption and decryption technology;

WHEREAS, Content Participant has reviewed Vidi and the Compliance Rules and the provisions of this Agreement, believes them to be appropriate, and wishes to obtain the status of third party beneficiary on the basis of the terms and conditions set forth in this Agreement;

NOW, THEREFORE, in consideration of the foregoing, and of the mutual obligations and covenants set forth herein, and for other good and valuable consideration, the Parties agree and intend to be bound as follows:

Article 1 – Definitions and Terminology

1.1 Roles Applicable to Company

In this Agreement, except where the context clearly requires otherwise, the terms 'Content Participant', 'Implementer', 'Developer', 'Hardware Implementer', 'Software Implementer', 'Replicator', 'Master Manufacturer' or 'Component Implementer' (the foregoing terms collectively called "Roles"), each refers to Company, if Company has elected, by placing a mark in the applicable box on page 1 of this Agreement, to enter into this Agreement and obtain the rights and be subject to the obligations that apply to such Role. Where the context clearly so requires (e.g., in Sections 2.3, 2.5, ---), the terms may be used to refer to other parties who have agreed to performing the respective Roles under their Vidi Content Protection Agreement.

1.2 Definitions

"Administration Fee" means the fees for handling orders for Keys and for shipping Keys, as specified in the Vidi Key Order Form (Exhibit B).

"Affiliate" means, with respect to Philips, HP or Company, any business entity (i) owned or controlled by Philips, HP or Company, respectively, (ii) owning or controlling Philips, HP or Company, respectively, or (iii) owned or controlled by the business entity owning or controlling Philips, HP or Company, respectively, at the material time. For the purposes of this definition a business entity shall be deemed to own or to control another business entity if more than 50% (fifty per cent) of the voting stock of the latter business entity, ordinarily entitled to vote in the election of directors (or, if there is no such stock, more than 50% (fifty per cent) of the ownership of or control in the latter business entity) is held by the owning or controlling business entity.

"**Applicable Revocation Criteria**" means (i) the revocation criteria defined in Section D.1 for Revocation of Hardware Device Keys, or (ii) the revocation criteria defined in Section D.2 for Revocation of Software Device Keys.

"Application Key Block" means a cryptographic data structure, needed by a Software Playback Function in the process of authenticating a Data Drive, as described in the Specification.

"APS Trigger Bit" means information associated with audiovisual content that indicates that an automatic gain control or color stripe technology, as listed in Section A.1.2.3, shall be applied on any analog output that transmits such audiovisual content.

"Authorized Employee" means an employee of Company who is (i) authorized by Company to receive Highly Confidential Information, and (ii) has signed the acknowledgement form (Exhibit E).

"Broadcast Flag" means the redistribution control descriptor (rc_descriptor()) described in ATSC A/65B: "Standard: Program and System Information Protocol for Terrestrial Broadcast and Cable (Revision B)", which signals that broadcast video may be recorded but must be protected against redistribution.

"CableLabs" means Cable Television Laboratories, Inc.

"CCI" or **"Copy Control Information"** means the information reflecting the states Copy Never, Copy One Generation, Copy No More, and EPN, as such information is defined by the source of the rules that mandate the application of encryption technology (e.g., (i) the law of the territory where a video recording product is sold, (ii) the rules governing the handling of content through a particular protected source, or (iii) the format or patent license for the recording technology).

"CCI-MAC" shall have the meaning defined in the Specification.

"Company" means the entity identified on the first page of this Agreement.

"Company Confidential Information" means information defined as "Company Confidential Information" in Section 8.2.

"Compliance Rules" means the compliance and robustness requirements set forth in Exhibit A, as such Exhibit may be amended from time to time pursuant to Article 6.

"Compliant Vidi Product" comprises (i) (a) Vidi Discs, Vidi Stampers, and Vidi Masters that conform to the Specification, and (b) Vidi Recorder/Player Products that use Vidi in accordance with the Specification to encrypt or decrypt audiovisual content only within the Field of Use, that (ii) comply with the Compliance Rules, and that and otherwise satisfy the terms and conditions of this Agreement.

"Computer" means a general-purpose computing device that allows its user to install a wide variety of commercially available software applications.

"Confidential Information" means information defined as "Confidential Information" in Section 8.1.

"Copy Never" means the CCI status that indicates that audiovisual content labeled with this status may not be copied.

"Copy No More" means the CCI status that indicates that audiovisual content labeled with this status is a first generation copy made from audiovisual content labeled as Copy One Generation, and shall not be copied further.

"Copy One Generation" means the CCI status that indicates that audiovisual content labeled with this status may be copied but that such copy shall not itself be copied.

"Data Drive" means an optical data drive for use in a Computer that implements the interface as defined in chapter 7 of the Specification.

"Decrypted Audiovisual Data" means decrypted Encrypted Audiovisual Data, including decrypted Encrypted Audiovisual Data that has been decompressed, re-compressed, scaled, and/or otherwise processed after decryption. With respect to any particular Vidi Recorder/Player Product, Decrypted Audiovisual Data does not include content after it has been transmitted from such Product pursuant to sections A.1.2.1 or A.1.2.2. of the Compliance Rules.

"Device Key" means the set of cryptographic keys, referred to in the Specifications as a "set of Node Keys", that (i) must be embedded in each Playback Function and Recording Function to enable decryption and encryption of audiovisual content and (ii) must be embedded in a Data Drive to enable authentication with Software Recording Functions and Software Playback Functions.

"**DFAST License Agreement**" means the "DFAST Technology License Agreement for Unidirectional Digital Cable Products" as offered by CableLabs.

"Disc Key Block" or **"DKB"** means a data structure that is embedded in a DVD+RW or DVD+R Disc which, in combination with Device Keys embedded in a Playback Function, enables such Playback Function to decrypt data from such DVD+RW or DVD+R Disc, and in combination with Device Keys embedded in a Recording Function, enables such Recording Function to encrypt audiovisual content on such DVD+RW or DVD+R Disc in accordance with the Specification.

"DVD+RW Recorder Content Protection Agreement" shall mean the content protection agreement offered by Philips with the patent license agreement for the DVD+RW technology.

"Eligible Content Participant" shall mean a Content Participant who meets the criteria set out in Section 9.3.

"Encrypted Audiovisual Data" means audiovisual content that is encrypted using Vidi.

"EPN" means the CCI used to indicate that content is to be protected with an approved encryption technology, but that copy control restrictions are not being asserted over such content. By way of example, and without limitation, the EPN status may be used to indicate video content that is protected by the Broadcast Flag.

"FCC" means the United States Federal Communications Commission.

"Field of Use" means: (i) the use of Vidi to encrypt audiovisual content for recording on DVD+R and DVD+RW optical discs and (ii) the use of Vidi to decrypt Encrypted Audiovisual Data for playback from such discs, and (iii) embedding a DKB in Vidi Masters, Vidi Stampers, and Vidi Discs in order to permit the foregoing, all in accordance with the Specification and the Compliance Rules.

"Hardware Device Key" means a Device Key for use in a Hardware Playback Function, Hardware Recording Function, or a Data Drive.

"Hardware Implementation" means an implementation of all, or part, of the Specification that cannot be modified by users without changing the hardware by, by means of example and without limitation, replacing ICs or adding new ICs.

"Hardware Playback Function" means a Playback Function that is not a Software Playback Function. For the purpose of clarification and without limitation, a Hardware Playback Function may be implemented partially or completely in software or firmware that runs on a computing device that does not allow its user to install widely available commercial software applications.

"Hardware Recording Function" means a Recording Function that is not a Software Recording Function. For the purpose of clarification and without limitation, a Hardware Recording Function may be implemented partially or completely in software or firmware that runs on a computing device that does not allow its user to install widely available commercial software applications.

"Highly Confidential Information" means the information defined in Section 8.3 as "highly confidential".

"Key Fees" means the fees specified in Section 3.3.

"Keys" comprises Application Key Blocks, Device Keys, Licensed Constant 1, Licensed Constant 2, and DKBs.

"Licensed Constant 1" means a cryptographic key, referred to in the Specifications as "Initialization Vector 1", needed by Playback Functions and Recording Functions.

"Licensed Constant 2" means a cryptographic key, referred to in the Specifications as "Initialization Vector 2", needed by Software Recording Functions, Software Playback Functions and Data Drives.

"Navigation Pack" shall have the meaning defined in the Specification.

"Necessary Claims" means claims of a patent or patent application that must be infringed in order to use Vidi in the Field of Use in compliance with the Specification and Compliance Rules, which is owned by Philips, HP or Company. Necessary Claims do not include any intellectual property other than that specifically directed to Vidi and, without limitation, specifically do not include underlying intellectual property, included in the Specification only be reference, such as intellectual property pertaining to semiconductor technology, tamper-resistance technology, the creation or replication of optical media or other media for the distribution of audio, audiovisual or textual information or to the means of reading or writing to such optical media or other media.

"Playback Function" means the functionality implementing the decryption of Encrypted Audiovisual Data.

"Recording Function" means the functionality implementing the encryption of audiovisual content in accordance with the Specification.

"Revocation", **"Revoke"** or **"Revoked"** means the procedure by which Keys embedded in a Vidi Recorder/Player Product may be invalidated, rendering: (i) the Playback Function in such Vidi Recorder/Player Product unable to decrypt Encrypted Audiovisual Data, (ii) the Recording Function in such Vidi Recorder/Player Product unable to record Encrypted Audiovisual Data on Vidi Discs, or (iii) a Data Drive unable to perform authentication with a Software Playback Function.

"Software Device Key" means a Device Key for use in a Software Playback Function or Software Recording Function.

"Software Playback Function" means a Playback Function, implemented as a software application, running on a Computer that receives Encrypted Audiovisual Data from a Data Drive.

"Software Recording Function" means a Recording Function, implemented as a software application, running on a Computer, that records Encrypted Audiovisual Data on a Data Drive.

"Specification" means the document entitled "Vidi Copy Protection System for the DVD+R/+RW Video Recording Format; System Description; Version 1.0" and subsequent updates or modifications thereof made in accordance with the terms of this Agreement.

"Unique ID" shall have the meaning defined in Section 6.3.2 of the Specification.

"Vidi" means the system for encrypting and decrypting certain digital audiovisual content recorded on DVD+RW and DVD+R optical digital media as described in the Specification.

"Vidi Component" means a hardware or software component for use in a Vidi Recorder/Player Product that implements all or part of Vidi as defined in the Specification, and that is not a Compliant Vidi Product itself.

"Vidi Disc" means a DVD+R or DVD+RW disc, containing a DKB, that can be used for recording Encrypted Audiovisual Data.

"Vidi Intellectual Property" means Philips' and HP's Necessary Claims, know-how, and copyrights that Philips provides pursuant to this Agreement, to enable Implementer to use Vidi as permitted hereby in the Field of Use in accordance with the Specification and Compliance Rules. For the purpose of clarification, Vidi Intellectual Property does not include any intellectual property other than that specifically directed to Vidi and, without limitation, specifically does not include underlying intellectual property, included in the Specification only by reference, such as intellectual property pertaining to semiconductor technology, tamper-resistance technology, the creation or replication of optical media or other media for the distribution of audio, audiovisual or textual information or to the means of reading or writing to such optical media or other media.

"Vidi Key Order Form" means the form used for ordering Keys, as described in Exhibit B.

"Vidi Master" means a disc shaped physical object containing an encoded DKB in accordance with the Specifications, which is a template to generate a set of physical objects that are exact duplicates or negative images of the Vidi Master. Vidi Masters are used to manufacture Vidi Stampers.

"Vidi Product" comprises (a) Data Drives (b) Vidi Masters, (c) Vidi Stampers, (d) Vidi Discs, and (e) products containing (i) a Software Playback Function, (ii) a Software Recording Function, (iii) a Hardware Playback Function, or (iv) a Hardware Recording Function.

"Vidi Recorder/Player Product" comprises (a) Data Drives, and (b) products containing (i) a Software Playback Function, (ii) a Software Recording Function, (iii) a Hardware Playback Function, or (iv) a Hardware Recording Function.

"Vidi Stamper" means a disc shaped physical object which is a duplicate or negative image of a Vidi Master containing an encoded DKB in accordance with the Specifications, and which

may be used in injection moulding machines that replicate Vidi Discs. Vidi Stampers, provided that such stampers are manufactured, directly or indirectly, using a Vidi Master as the template, include so-called "father" and "mother' stampers, and moulds, which are used in injection moulding machines for replication of Vidi Discs.

Article 2 – Undertaking Not to Assert and Licenses

2.1 Undertaking not to assert.

2.1.1 Hardware Implementer

Subject to the terms and conditions of this Agreement, Philips hereby undertakes that it and its Affiliates shall not assert against Hardware Implementer and its Affiliates, the Vidi Intellectual Property, with respect to the use of Vidi Intellectual Property by Hardware Implementer and its Affiliates in the Field of Use to develop, make, have made, use, sell, offer for sale, import, export, transfer or otherwise dispose of (i) Vidi Components in accordance with the Specifications, (ii) Data Drives in accordance with the Specification and Compliance Rules, and (iii) products that contain a Hardware Playback Function, a Hardware Recording Function, or both, in accordance with the Specification and Compliance Rules. Philips has been authorized by HP to confirm to Company that HP undertakes that it and its Affiliates shall not assert against Hardware Implementer and its Affiliates, the Vidi Intellectual property under the same conditions. Hardware Implementer acknowledges and agrees that in order to manufacture Data Drives or products containing a Hardware Playback Function or a Hardware Recording function, it is necessary to obtain Hardware Device Keys from Philips.

2.1.2 Software Implementer

Subject to the terms and conditions of this Agreement, Philips hereby undertakes that it and its Affiliates shall not assert against Software Implementer and its Affiliates, the Vidi Intellectual Property, with respect to uses of the Vidi Intellectual Property by Software Implementer and its Affiliates in the Field of Use to develop, make, have made, use, sell, offer for sale, import, export, transfer and otherwise dispose of (i) Vidi Components in accordance with the Specifications or (ii) products containing a Software Playback Function or a Software Recording Function, in accordance with the Specification and Compliance Rules. Philips has been authorized by HP to confirm to Company that HP undertakes that it and its Affiliates shall not assert against Software Implementer and its Affiliates, the Vidi Intellectual property under the same conditions. Software Implementer acknowledges and agrees that in order to use Vidi, it is necessary to obtain Software Node Keys and Application Key Blocks from Philips.

2.1.3 Replicator

Subject to the terms and conditions of this Agreement, Philips hereby undertakes that it and its Affiliates shall not assert against Replicator and its Affiliates, the Vidi Intellectual Property, with respect to uses of the Vidi Intellectual Property by Replicator and its Affiliates in the Field of Use to make, use, sell, offer for sale, import, export, transfer and otherwise dispose of Vidi Discs in accordance with the Specification. Philips has been authorized by HP to confirm to Company that HP undertakes that it and its Affiliates shall not assert against Replicator and its Affiliates, the Vidi Intellectual property under the same conditions. For the purpose of clarification and the avoidance of doubt, the undertaking not to assert as given in this Section 2.1.3 does not cover the use of Vidi

Intellectual Property to make, have made, use, sell, offer for sale, import, export, develop and distribute Vidi Masters or Vidi Stampers.

2.1.4 Master Manufacturer

Subject to the terms and conditions of this Agreement, Philips hereby undertakes that it and its Affiliates shall not assert against Master Manufacturer and its Affiliates, the Vidi Intellectual Property, with respect to uses of the Vidi Intellectual Property by Master Manufacturer and its Affiliates in the Field of Use to make, use, sell, offer for sale, import, export, transfer and otherwise dispose of Vidi Masters or Vidi Stampers in accordance with the Specification and Compliance Rules, provided that Master Manufacturer is in full compliance with the provisions of Section 3.3.4. Philips has been authorized by HP to confirm to Company that HP undertakes that it and its Affiliates shall not assert against Master Manufacturer and its Affiliates, the Vidi Intellectual property under the same conditions. For the purpose of clarification and for the avoidance of doubt, the undertaking not to assert given in this Section 2.1.4 does not cover the use of Vidi Intellectual Property to make, have made, use, sell, offer for sale, import, export, develop and distribute Vidi Discs.

2.1.5 Component Implementer

Subject to the terms and conditions of this Agreement, Philips hereby undertakes that it and its Affiliates shall not assert against Component Implementer and its Affiliates, the Vidi Intellectual Property, with respect to uses of the Vidi Intellectual Property by Component Implementer and its Affiliates in the Field of Use to develop, make, have made, use, sell, offer for sale, import, export, transfer and otherwise dispose of Vidi Components in accordance with the Specification, provided that such Vidi Components shall not contain Device Keys. Philips has been authorized by HP to confirm to Company that HP undertakes that it and its Affiliates shall not assert against Component Implementer and its Affiliates, the Vidi Intellectual property under the same conditions. For the purpose of clarification and for the avoidance of doubt, the undertaking not to assert given in this Section 2.1.5 does not cover the use of Vidi Intellectual Property to make, have made, use, sell, offer for sale, import, export, develop and distribute Vidi Recorder/Player Products.

2.1.6 Content Participant

Subject to the terms and conditions of this Agreement, Philips hereby undertakes that it and its Affiliates shall not assert against Content Participant and its Affiliates, the Vidi Intellectual Property, with respect to the use of Vidi Intellectual Property by Content Participant or its Affiliates in the Field of Use (ii) for Content Participant's or its Affiliates' using or causing the use of Vidi to protect its or their audiovisual content within and limited to the Field of Use. Philips has been authorized by HP to confirm to Company that HP undertakes that it and its Affiliates shall not assert against Content Participant and its Affiliates, the Vidi Intellectual property under the same conditions.

2.2 Development Only.

Subject to the terms and conditions of this Agreement, Philips hereby undertakes that it and its Affiliates shall not assert against Developer and its Affiliates, the Vidi Intellectual Property, with respect to uses of the Vidi Intellectual Property by Developer to develop Vidi Components and Vidi Products in accordance with the Specification. Philips has been authorized by HP to confirm to Company that HP undertakes that it and its Affiliates shall not assert against Developer and its Affiliates, the Vidi Intellectual property under the same conditions. Developer acknowledges and agrees that the undertaking not to assert given in this Section 2.2 expressly does not extend to any

right to make, have made, sell, offer for sale, import, export, transfer or otherwise dispose of Vidi Products and Vidi Components.

2.3 Limitations on the Distribution of Vidi Stampers, Vidi Masters, and Vidi Components.

2.3.1 Vidi Stampers

Vidi Stampers shall not be sold, transferred or otherwise disposed of except to Co-Implementers who are Replicators or Master Manufacturers. Replicator shall only procure Vidi Stampers from Co-Implementers who are Master Manufacturers.

2.3.2 Vidi Masters

Vidi Masters shall not be sold, transferred or otherwise disposed of except to Co-Implementers who are Master Manufacturers.

2.3.3 Vidi Components

Vidi Components containing an embedded Device Key, shall not be sold, transferred, or otherwise disposed of, except to Co-Implementers who are Hardware Implementers or Software Implementers.

2.4 Compliance with Specifications and Compliance Rules

Implementer shall use Vidi only in accordance with the Specifications, and agrees to be subject to the requirements of the Specifications.

Implementer shall cause each Vidi Recorder/Player Product that it makes, has made, sells, transfers, or otherwise disposes of, to comply with the Compliance Rules, and agrees to be subject to the requirements of the Compliance Rules.

If Philips engages in any activity within the scope of any of the Roles of Implementer, Philips agrees that, within the Field of Use, it will be subject to the obligations of Section 2.4. Philips has been authorized by HP to confirm that HP shall, within the scope of any of the Roles of Implementer and within the Field of Use, similarly be subject to the obligations of Section 2.4. Further, Philips and HP may be treated as Replicator, Master Manufacturer, Hardware Implementers and Software Implementers for the purpose of Sections 2.3.1, 2.3.2, 2.3.3 and 9.3.2. This provision shall not create any rights in favor of any Co-Implementer against Philips or HP, and shall create only those rights in favor of Content Participants as are granted by Section 9.3.2.

2.5 Reciprocal Licensing Covenant.

Company shall, and shall cause each of its Affiliates to, grant licenses under its and its Affiliates' Necessary Claims, on reasonable, non-discriminatory terms, (i) to Philips and its Affiliates and to HP and its Affiliates, for the granting of the rights granted under Vidi Content Protection Agreements and for the making, having made, using, importing, offering for sale, selling, and distribution of Vidi Products and Vidi Components within and limited to the Field of Use, (ii) and to all those entities who are Co-Implementers and their Affiliates, who have agreed to the licensing obligations set forth in this Section 2.5 under their respective Necessary Claims, for the making, having made, using, importing, offering for sale, selling, and distribution of Compliant Vidi Products and Vidi Components within and limited to the Field of Use and, further, with respect to any particular Co-Implementer, limited to the Role established under that Co-Implementer's Vidi Content Protection

Agreement, and (iii) to all those entities who are Content Participants and their Affiliates who have agreed to the licensing obligations set forth in this Section 2.5 under their respective Necessary Claims, for the using or causing the use of Vidi to protect its or their audiovisual content within and limited to the Field of Use. The undertaking set out in the preceding sentence shall not extend to features of a product which are not required to comply with the Specification or for which there exists a non-infringing commercially feasible alternative. Further, such promise shall not extend in favor of any person or entity which has (or the Affiliate of which has) refused to grant such a license or give an undertaking not to assert to Company provided that Company (x) is not willfully in material breach of its obligations under this Agreement, including the Compliance Rules, and (y) is not otherwise in material breach of this Agreement, including the Compliance Rules, which breach has not been cured or is not capable of cure within 30 days of Company's receipt of notice thereof.

Article 3 – Fees And Deliverables

3.1.a Fees and Deliverables for Implementers.
Upon execution of this Agreement, Implementer shall pay Philips a non-refundable, non-recoupable fee of € 5,000 (five thousand Euros) without any deduction whatsoever, whether for bank transmission charges or otherwise. Within 21 days after receipt by Philips of said amount of € 5,000, Philips shall cause to be delivered to Implementer at the address specified in the notice provision of this Agreement (Section 13.5) a copy of the Specification. A single copy of any future revised versions and updates of the Specification as well as such related documents as may be provided to Implementer pursuant to Section 6.3 will be delivered by Philips to Implementer free of charge for use by Implementer during the term of this Agreement and in accordance with its provisions.

At the request of Hardware Implementer, Software Implementer, or Component Implementer, and after receipt of the fee of € 5,000 set forth in this Section 3.1.a, Philips shall cause to be delivered at the address specified in the notice provision of this Agreement (Section 13.5), Licensed Constant 1 and Licensed Constant 2.

3.1.b Fees and Deliverables for Content Participants.
In consideration of the rights granted to Content Participant and the undertakings given by Philips as set out herein, Content Participant agrees to pay to Philips a yearly, non-refundable, non-recoupable fee of € 10,000 (ten thousand Euros). The first payment of such yearly fee shall be due within 14 days after the date of the Agreement and the subsequent yearly fees shall be payable on March 1 of the year following the year in which this Agreement has been entered into and on March 1 of each subsequent year thereafter. In the event that, at any time during the term of this Agreement, Content Participant fails to pay the yearly fee in accordance with the provisions hereof, Philips shall notify Content Participant of such omission, in writing. Content Participant shall remedy its failure to pay the yearly fee within 30 days from receipt of said written notification and only the failure to pay the yearly fee within said 30-day period shall constitute a breach by Content Participant of its obligation to pay the yearly fee under this Section 3.1.b. Within 21 days after receipt by Philips of the first payment, Philips shall cause to be delivered to Content Participant at the address specified in the notice provision of this Agreement (Section 13.5) a copy of the Specification. A single copy of any future revised versions and updates of the Specification as well as such related documents as may be provided to Content Participant pursuant to Section 6.3 will be

delivered by Philips to Content Participant without additional charge for use by Content Participant during the term of this Agreement and in accordance with its provisions.

3.2 Key Ordering.

This Section 3.2 is applicable only if Company is an Implementer but not a Developer or a Replicator.

Implementer shall order and pay to Philips the fees for Keys set forth in Section 3.3. as well as Administration Fees set forth on the Vidi Key Order Form in accordance with the terms and conditions set forth in the Vidi Key Order Form, as published by Philips on its website *www.licensing.philips.com*, provided that changes in the Key Order Form from that attached hereto as Exhibit B shall be limited to (i) an increase in such Administration Fees over time that shall not exceed an amount commensurate with any increase in Philips' costs of shipping Keys and handling an order, (ii) commercially reasonable changes in the procedures for ordering, payment and delivery of keys, (iii) commercially reasonable changes in the time between receipt of a Key Order Form together with the corresponding payment and the delivery of Keys at Implementer's contact address, (iv) commercially reasonable changes in the payment method, and (v) commercially reasonable changes in the number of Keys per distribution disc. Without limiting the foregoing, where costs per Co-Implementer decrease, Philips shall use commercially good faith efforts to reduce the Administration Fee. Implementer acknowledges that the Vidi Key Order Form in Exhibit B of this Agreement is attached for informational purposes and that the only valid form and terms and conditions shall be those as published by Philips on its website. Implementer acknowledges and confirms that Keys delivered hereunder remain the property of Philips, and that therefore, Implementer is not allowed to redistribute, sell or otherwise transfer Keys to another Implementer or any third party, except as expressly permitted under Section 8.4.3, and that Philips will have the right to Revoke any Device Key in accordance with the Revocation Procedures in Article 7 and Exhibit D.

3.3 Key Fees and Conditions for Using Keys.

3.3.1 Hardware Implementers

Hardware Implementer shall (i) embed, or cause to be embedded, a different Hardware Device Key in each of Hardware Implementer's products containing a Hardware Playback Function, a Hardware Recording Function or both, and (ii) embed, or cause to be embedded, a different Hardware Device Key in each of Hardware Implementer's Data Drives. In addition to the applicable Administration Fee, Hardware Implementer shall pay to Philips an amount of € 0.05 (five Euro cents) per Hardware Device Key ordered.

3.3.3 Software Implementers

Software Implementer shall embed Software Device Keys and Application Key Blocks in each of Software Implementer's products (i) containing a Software Recording Function, a Software Playback Function, or both. To obtain said Software Device Keys and Application Key Blocks, Software Implementer shall pay Philips the applicable Administration Fee.

3.3.4 Master Manufacturers

Master Manufacturer shall embed a different Disc Key Block in each of Master Manufacturer's Vidi Masters. To obtain said Disc Key Blocks, Master Manufacturer shall pay Philips the applicable Administration Fee.

3.3.5 Replicators

As part of the consideration for the right to embed DKBs in its Vidi Discs, Replicator shall pay to Philips € 0.01 (one Euro cent) per Vidi Disc manufactured. To establish the amounts due, Replicator shall report and pay to Philips in accordance with the provisions of Section 4.1 and 4.2.

Article 4 – Reporting And Payment By Replicator

4.1. Reporting by Replicator.

Within 30 days following 31 March, 30 June, 30 September and 31 December of each year during the term of this Agreement, Replicator shall submit to Philips (even in the event that no sales have been made) a written statement in the form as attached hereto as Exhibit C (Key Fee Reporting Form), signed by a duly authorized officer on behalf of Replicator specifying the number of Vidi Discs manufactured and sold, transferred or otherwise disposed of by Replicator.

4.2. Payment by Replicator.

Replicator shall pay the Key Fees due to Philips within 60 days after the end of each quarter of each year during the term of this Agreement, in such country and in such currency as Philips may specify.

Within 30 days following the expiration or termination of this Agreement, Replicator shall submit to Philips a certified report on the number of Vidi Discs in stock at the time of expiration or termination of this Agreement. Key Fees, calculated in accordance with Section 3.3.5, shall be due and payable on all such Vidi Discs manufactured prior to, but remaining in stock with Replicator on the date of expiration or termination of this Agreement.

Any payment under this Agreement which is not made on the date(s) specified herein, shall accrue interest at the rate of 2% (two per cent) per month (or part thereof) or the maximum amount permitted by law, whichever is lower.

All costs, stamp duties, taxes and other similar levies arising from or in connection with the conclusion of this Agreement shall be borne by Replicator. In the event that the government of a country imposes any income taxes on payments by Replicator to Philips hereunder and requires Replicator to withhold such tax from such payments, Replicator may deduct such tax from such payments. In such event, Replicator shall promptly provide Philips with tax receipts issued by the relevant tax authorities so as to enable Philips to support a claim for credit against income taxes which may be payable by Philips or its Affiliates in The Netherlands and to enable Philips to document, if necessary, its compliance with tax obligations in any jurisdiction outside The Netherlands.

Article 5 – Records and Audit Rights

5.1. Maintenance and Retention of Records.

In order that (i) the statements to be provided by Replicator pursuant to Section 4.1., and (ii) the proper installation and use of Keys, payment of Key Fees, the proper disposal of Vidi Products and Vidi Components under this Agreement by Hardware Implementers and Master Manufacturers, may be verified, Hardware Implementer, Replicator, and Master Manufacturer shall keep complete and

accurate books and records relating to the manufacture and sale, transfer or other disposal of Vidi Products and Vidi Components, insofar such Vidi Components contain Hardware Device Keys, the installation of Hardware Device Keys into Vidi Products and Vidi Components (in the case of Hardware Implementer), and the procurement of Vidi Stampers for the manufacture of Vidi Discs (in the case of Replicator) and the installation of DKBs into Vidi Masters (in the case of Master Manufacturer). Hardware Implementer, Replicator, and Master Manufacturer shall keep such books and records available for a period of 5 years following the latest of the last manufacture, sale, transfer or other disposal of the Vidi Product or Vidi Component to which such books and records pertain.

5.2. Right to Audit.

Philips shall have the right from time to time to appoint one or more independent, certified public auditors, who is (are) not related to Philips or HP, to inspect Implementer's books and records only to the extent and for the sole purpose of verifying:

a. In the case of Hardware Implementer, that (i) each product containing a Hardware Playback Function or a Hardware Recording Function contains a different Hardware Device Key, (ii) each Data Drive contains a different Hardware Device Key, and (iii) each Vidi Component containing a Hardware Device Key has been disposed of in accordance with Section 2.3.3;

b. In the case of Master Manufacturer, that (i) each Vidi Master contains a different DKB, (ii) each Vidi Master has been disposed of in accordance with Section 2.3.2 and (ii) each Vidi Stamper has been disposed of in accordance with Section 2.3.1;

c. In the case of Replicator, that (i) the statements submitted in accordance with Section 4.1 are true and correct, (ii) that information provided in accordance with Section 7.4 is true and correct, and (iii) that each Vidi Stamper used for embedding the DKBs has been procured from entities that are Master Manufacturers in accordance with Section 2.3.1.

5.3 Procedures for Audit.

Any inspection conducted pursuant to Section 5.2. shall take place no more than once per calendar year and shall be conducted in a commercially reasonable manner. Philips shall obligate the auditors to comply with the confidentiality requirements of Section 8.2 with respect to Company Confidential Information disclosed by Implementer in the course of such audit. Philips shall give Implementer written notice of such inspection at least 7 days prior to the inspection. Implementer shall willingly co-operate and provide all such assistance in connection with such inspection as the auditors may require. The inspection shall be conducted at Philips's own expense, provided that in the event that any deficiency in payment or in the reporting of payments due to Philips exceeding 5% (five per cent) of the amount that should have been paid or reported had this Agreement been fully complied with, or in the event that the audit reveals a Material Breach by Implementer that is subject to Liquidated Damages under section 9.2, the reasonable cost of the inspection shall be borne by Implementer, without prejudice to any other claim or remedy as Philips may have under this Agreement or under applicable law. Philips's right of inspection, as set out in this Section shall survive termination or expiration of this Agreement.

5.4 Inapplicability of this Article.

This Article 5 shall not apply to Implementer in the Role of Developer, Software Implementer or Component Implementer.

Article 6 – Change Procedures Regarding Specification And Compliance Rules

6.1 Limitation of Changes in Specification and Compliance Rules.

Philips shall not make changes in the Specification or Compliance Rules except as permitted by this Article 6, pursuant to the procedure set forth in this Article 6.

6.2 Permitted Changes.

6.2.1 Errors, Omissions and Bug Fixes.

Philips may clarify ambiguities in the Specification and Compliance Rules and may correct (i) typographical errors or similar mistakes in the Compliance Rules and Specifications, and (ii) any bugs, or other technical defects in Vidi, as long as such correction or clarification does not (a) materially amend or alter Vidi or expand Vidi functionality, (b) impose new limitations on the functionality of Compliant Vidi Products, or (c) materially increase the cost or burden of implementing Vidi.

6.2.2 Additional Analog Outputs.

Philips may make changes to add additional analog copy control labeling technologies and permitted analog outputs in Compliance Rule Section A.1.2.1, as long as such additional technologies or outputs provide protection to commercially audiovisual content protected using Vidi that is no less robust than another technology identified in (a) said Section, (b) the DFAST License Agreement, (c) section 6.2.1.1 of the Procedural Specification for CSS as established by the DVD Copy Control Association, or (d) any rule that may be adopted by the FCC to govern analog outputs for commercial audiovisual content.

6.2.3 Changes to Conform to a Government Mandate.

Philips may make changes in the Specification and Compliance Rules applicable within the territory of a competent governmental authority (i) in order to comply with a requirement established by such governmental authority within the territory, or (ii) if such change is necessary in order to qualify as an authorized technology for use with the recording of commercial audiovisual content pursuant to a regulatory regime established or supervised by such governmental authority.

6.3 Procedure for Changes.

6.3.1 Announcement of a Proposed Change.

Philips shall notify Company in writing if a proposed change ("Proposed Change") of the Specification or Compliance Rules is under serious consideration by Philips. The notice will provide the details of the change under consideration and the rationale for the change.

6.3.2 Announcement of a Draft Change.

Not less than 90 days after the announcement of a Proposed Change, Philips shall notify Company in writing if Philips intends to adopt the Proposed Change in either its original form or in revised form, based on comments received or further consideration. The notice will provide the details of

the change that Philips intends to make ("Draft Change") and the rationale for any difference between the Draft Change and the Proposed Change.

6.3.3 Consultation.
Philips will permit Company to comment on a Proposed Change and Draft Change at any time after announcement of the change. Philips will respond to and attempt to reconcile substantive comments from Company, Co-Implementers and Content Participants, and will, at the request of Company, meet with Company to discuss the Proposed Change or Draft Change.

6.3.4 Modification of the Draft Change.
Philips may modify a Draft Change, based on comments or discussions with Company, Co-Implementers or Content Participants. Philips shall notify Company in writing about any such modification to a Draft Change. The notice will provide the details of the modified Draft Change and the rationale for any difference between the modified Draft Change and the previously announced Draft Change.

6.3.5 Arbitration.
If Company objects to a Draft Change, and consultation pursuant to Section 6.3.3 does not result in an acceptable modification of the Draft Change, Company may seek arbitration, no later than 30 days after Philips' announcement of a Draft Change to which Company objects, by (i) providing Philips with written notice, at the address specified in the notice provision of this Agreement (Section 13.5), and (ii) submitting the request for arbitration to a neutral arbiter skilled in law and the applicable technology in accordance with the provisions of this Section 6.3.5 and the general provisions for arbitration as specified in Exhibit F. Philips shall notify Company in writing when a Co-Implementer or Content Participant has sought arbitration in accordance with the provision of this Section 6.3.5.

The disagreement between Company (the "Requesting Party") and Philips about a Draft Change shall be settled by arbitration administered by the American Arbitration Association in accordance with its Commercial Arbitration Rules including its Supplementary Procedures for online Arbitration (as published by the American Arbitration Association on its website http://www.adr.org/), and judgment on the award rendered by the arbitrator(s) may be entered in any court having jurisdiction thereof.

The parties to the arbitration shall be the Requesting Party, and Philips (collectively, the "Arbitration Parties").

Any Company with an interest in the Draft Change shall have the right to join in the arbitration as a party (either supporting or opposing the Draft Change) within 30 days after the request for arbitration was submitted to the American Arbitration Association. Only one arbitration action may be brought against Philips in relation to any particular Draft Change.

The Requesting Party and other parties opposing the Draft Change shall bear the burden of proving, by a preponderance of the evidence, that the Draft Change does not meet the criteria for Permitted Changes set forth in Section 6.2. The arbitrator(s) is (are) empowered solely to determine whether the Draft Change meets the criteria set forth in Section 6.2.

Philips shall not apply a Draft Change if the arbitrator(s) determine(s) that such Draft Change does not comply with Section 6.2. Philips may apply a Draft Change if the arbitrator(s) determine(s) that such Draft Change complies with Section 6.2.

In the event that the arbitrators fail to reach a decision within 180 days after submission of the request for arbitration, the change shall be deemed approved and the arbitration shall be terminated. The foregoing 180-day deadline may be extended by the arbitrator(s) only on the ground of unreasonable delay caused by Philips, and only for the time lost due to such delay.

In the event that the Requesting Party (and other parties to the arbitration opposing the change) and Philips reach agreement to modify the Draft Change, Philips shall provide notice to Company, Co-Implementers and Content Participants in accordance with Section 6.3.4, and the arbitration procedure shall be terminated.

6.3.6 Final Announcement of the Change.
A Draft Change in the Specification and Compliance Rules permitted by Section 6.2 may be adopted by Philips (i) after not less than 30 days have passed following the announcement of the Draft Change or the announcement of a modification of that Draft Change, and no arbitration has been commenced opposing the Draft Change, or (ii) following the conclusion or termination of all arbitration procedures that relate to the Draft Change, and the Draft Change is permitted pursuant to Section 6.3.5. Philips shall notify Company in writing that a Draft Change has been adopted.

6.3.7 Shortened Procedure for Non-Controversial Change.
The period of 90 days provided in Section 6.3.2 may be shortened to 30 days, and the period of 30 days provided in Sections 6.3.5 may be shorted to 15 days (collectively, "Shortened Periods") if Philips announces in its notice of a Proposed Change (as described in Section 6.3.1) that it believes the Proposed Change is non-controversial and that the Shortened Periods apply.

Notwithstanding the above, the Shortened Periods shall not apply in the event that two or more entities that are Implementers or Content Participants provide Philips with written notice, no later than 30 days after the announcement of Proposed Change and Shortened Periods by Philips and at the address specified in the notice provision of this Agreement (Section 13.5), that they object to the use of such Shortened Period for the Proposed Change. Philips shall, in such event, notify Company in writing that the normal periods, as specified in Sections 6.3.2 and 6.3.5, apply.

6.4 Implementation of Changes.
Implementer shall comply with all changes to the Specification and Compliance Rules that are permitted under Section 6.2, within 18 months after the notification by Philips of such amendments pursuant Section 6.3.6, or within such longer, reasonable, period as Philips may specify.

6.5 Enhancements and New Features.

6.5.1 Extensions.
Company is advised that it is possible that Philips will define extensions of Vidi or other encryption systems for audiovisual content that use a significant number of technical elements of the Specification ("Vidi Extensions"). For example and without limitation, such other encryption system may be (i) a system for encrypting other video formats on DVD+R and DVD+RW discs, (ii) a system for encrypting audiovisual content on other recording media, (iii) a system for encrypting

audio formats on DVD+R and DVD+RW discs, or (iv) a system for recording audiovisual content that is labeled with control information other than the CCI than is currently defined in this Agreement for Vidi. Company acknowledges that approval by the FCC may be required prior to the application of such Vidi Extension in the territory of the United States.

6.5.2 Notification and Offer.
Philips shall offer Company at least ninety (90) day's notice and opportunity to review and comment on any Vidi Extension and will make a good faith effort to reconcile comments and objections to any such extension. Philips shall offer any Vidi Extension to Company under a different agreement, or as an addendum to this Agreement.

Article 7 – Revocation

7.1 Generally.
The Specification includes means by which Keys that are embedded in Vidi Recorder/Player Products may be Revoked.

7.2 Right to Revoke.
Philips may revoke a Key (i) in accordance with the criteria and the procedure as set out in Exhibit D to this Agreement, and (ii) by order of a court of competent jurisdiction.

7.3 Obligations for Master Manufacturer after Revocation of a Device Key.
If and when Philips performs the Revocation of a Device Keys, all DKBs that are in Master Manufacturer's possession shall be expired. Upon such Revocation, Philips will notify Master Manufacturer of such expiration and upon such notification, Master Manufacturer shall within 30 days cease production of Vidi Masters and Vidi Stampers with an expired DKB. Upon Master Manufacturer's request, Philips shall replace unused DKBs that have expired with new DKBs. Philips shall replace such expired DKBs free of charge and without payment of any Administration Fee by Master Manufacturer.

7.4 Obligations for Replicator after Revocation of a Device Key.
Replicator shall, at the request of Philips, when Philips has reasonable grounds to suspect that a Vidi Stamper used by Replicator to manufacture Vidi Discs contains an expired DKB, provide Philips with the names of all Master Manufacturers from whom Replicator has procured Vidi Stampers.

7.5 Obligations for Software Implementer after Revocation of a Device Key.
If and when Philips performs the Revocation of a Device Key, all Application Key Blocks that are in Software Implementer's possession shall be expired. Upon such Revocation, Philips will notify Software Implementer of such expiration and upon such notification, Software Implementer shall within 60 days cease the release of new versions of Software Playback Functions and Software Recording Functions with such expired Application Key Blocks. Upon Software Implementer's request, Philips shall replace unused Application Key Blocks that have expired with new Application Key Blocks. Philips shall replace such expired Application Key Blocks free of charge and without payment of any Administration Fee by Software Implementer.

Article 8 – Confidentiality

8.1 Confidential Information

This Section 8.1 is applicable only to Hardware Implementer, Software Implementer, and Component Implementer.

Confidential Information under this Agreement shall be Licensed Constant 1 and Licensed Constant 2, provided by Philips to Implementer according to the provisions of Section 3.1a.

Implementer may disclose Confidential Information only to regular employees, and individuals retained as independent contractors subject to confidentiality obligations equivalent to those applicable to full-time employees of Company who need to know the Confidential Information to perform task that relate to this Agreement.

Company shall use, and shall ensure that those third parties who receive Confidential Information from Company use, the same degree of care to avoid unauthorized disclosure or use of Confidential Information as Company or such party, as the case may be, employs with respect to its comparably important confidential information, but in any event, no less than a reasonable degree of care.

8.2 Company Confidential Information

Company Confidential Information under this Agreement shall be (i) reports made by Replicators under Section 4.1, (ii) audit reports provided to Philips by the auditor under Section 5.1, and (iii) information on number of Keys ordered by Implementer.

Philips shall use any Company Confidential Information provided by Company to Philips under this Agreement solely to perform administrative functions that relate to this Agreement.

Philips may disclose Company Confidential Information only to (i) regular employees, and individuals retained as independent contractors subject to confidentiality obligations equivalent to those applicable to full-time employees of Philips, who need to know the Company Confidential Information to perform administrative functions that relate to this Agreement, or (ii) Philips' attorneys, auditors or other agents who owe Philips a duty of confidentiality and are bound to maintain such information in confidence as a result of such confidential relationship. Without limiting the foregoing, Philips shall not disclose Company Confidential Information to any regular employee or other individual who is directly or indirectly responsible for the manufacture, sale, transfer, or other disposal of Vidi Products, or products that compete with Vidi Products in the market.

Philips shall use, and shall ensure that those third parties who receive Company Confidential Information from Philips, use the same degree of care to avoid unauthorized disclosure or use of Company Confidential Information as Philips or such party, as the case may be, employs with respect to its comparably important confidential information, but in any event, no less than a reasonable degree of care.

Notwithstanding the foregoing, Philips may use Company Confidential Information in connection with any legal procedure arising from a breach, or perceived breach, of this Agreement, and generally, in order to protect its rights under this Agreement and at law, provided that Philips shall

take reasonable care to prevent disclosure of Company Confidential Information, such as, for example, by seeking suitable protective orders or by providing Company with the opportunity to seek suitable protective orders.

8.3 Highly Confidential Information

The only Highly Confidential Information under this Agreement shall be Device Keys.

Company shall use Highly Confidential Information (and tangible embodiments of any Highly Confidential Information) solely for purposes of its implementation of Vidi in accordance with the terms and conditions of this Agreement.

8.3.1 Procedures for Handling Highly Confidential Information.

Implementer shall employ procedures for safeguarding Highly Confidential Information at least as rigorous as Implementer employs for its own most highly confidential information. Such procedures shall include, at a minimum:

(1) Implementer shall maintain on its premises a secure location in which any and all Highly Confidential Information shall be stored;
(2) Any Highly Confidential Information stored in such a location shall be accessible only by Authorized Employees;
(3) Implementer shall keep a record of access of the Highly Confidential Information by Authorized Employees; and
(4) As long as Highly Confidential Information is not in use, such information shall be stored in a locked safe at such secure location.

8.3.2 Dissemination to Employees.

Implementer may disseminate Highly Confidential Information only to the strictest minimum possible number of regular full-time employees of Implementer: (i) who have an absolute need to know such Highly Confidential Information in order to enable Implementer to implement Vidi Products; (ii) who are bound in writing by obligations of confidentiality sufficient to protect the Highly Confidential Information in accordance with the terms of this Agreement, and (iii) who, prior to the disclosure of such Highly Confidential Information, have (x) been identified in writing by Implementer to Philips; and (y) read and executed the acknowledgement form attached as Exhibit E hereto (a copy of such executed acknowledgement to be sent to Philips at the address specified in Exhibit E); Implementer shall, at all times, cause Authorized Employees to strictly abide by their obligations hereunder and shall use the same efforts to enforce the confidentiality obligations of each Authorized Employee after the termination of his/her employment as Implementer uses to enforce with respect to Implementer's own similarly confidential information, provided, that Implementer shall not use less than reasonably expected efforts in such enforcement.

Notwithstanding any contrary provision, Implementer shall not disseminate any Keys to more than 3 Authorized Employees, unless Implementer has notified Philips in advance of its intention to increase the number of Authorized Employees to an additional increment of up to 3 such employees. Implementer may change such Authorized Employees by request to Philips, but in doing so shall abide by the terms of this Section 8.3.2.

8.3.3 Disclosure to Co-Implementers

Implementer may also disclose Highly Confidential Information to a Co-Implementer where (i) such Co-Implementer is providing services to Implementer, or where Implementer is providing services

to such Co-Implementer, pursuant to the right under Section 2.1 to "have made" Vidi Products, (ii) such Co-Implementer is authorized to possess such Highly Confidential Information and (iii) the employee to whom disclosure is made is an Authorized Employee. Prior to any disclosure pursuant to the preceding sentence, Implementer must assure itself that such Co-Implementer is, in fact, authorized to possess the Highly Confidential Information to be disclosed, that the employee to whom such disclosure is to be made is entitled to possess the Highly Confidential Information to be disclosed, and that the method to be used to disclose Highly Confidential Information is as secure as the methods used by Philips to disclose the same information to Implementer.

Article 9 – Remedies –Third Party Beneficiaries

9.1 Material Breach by Implementer

For the purpose of this Agreement, a "Material Breach" by Implementer shall be any one of the following breaches: (i) the sale, transfer or other disposal of Vidi Recorder/Player Products that fail to comply with the Compliance Rules (ii) the sale, transfer or other disposal of Vidi Stampers to entities that are not Replicators or Master Manufacturers, (iii) the sale, transfer or other disposal of Vidi Masters to entities that are not Master Manufacturers, (iv) the sale, transfer or other disposal of Vidi Components that contain an embedded Device Key to entities that are not Hardware Implementers or Software Implementers, (v) the sale, transfer or other disposal by Hardware Implementers of two or more Data Drives that contain an identical Device Key, (vi) the sale, transfer or other disposal by Hardware Implementers of products containing a Hardware Playback Function or a Hardware Recording Function where two or more of these products contain an identical Device Key, (vii) the manufacturing by Master Manufacturer of two or more Vidi Masters with an identical DKB in breach of the provisions of Section 3.3.4, (viii) the manufacture by Master Manufacturer of a Vidi Master containing an 'expired DKB' in breach of the provisions of Section 7.3, (ix) the release by Software Implementer of new versions of Software Playback Functions or Software Recording Functions containing an expired Application Key Block, in breach of the provisions of Section 7.4, and (x) a breach by Implementer of the provisions of Section 8.3 for protecting Highly Confidential Information.

9.2 Liquidated damages.

The Parties agree that the damages to Philips, Content Participants and Co-Implementers resulting from a Material Breach of this Agreement by Implementer are substantial and likely to be impossible to calculate. In the event of any such a Material Breach by Implementer that (i) involves the manufacture, sale, transfer or other disposal of Vidi Products that violate the Vidi Compliance Rules and as a result fail to protect Vidi protected content as contemplated hereby, (ii) involves the sale, transfer or other disposal of Vidi Components containing an embedded Device Key to entities that are not Hardware Implementers or Software Implementers, or (iii) involves a breach by Implementer of the provisions of Section 8.3 for protecting Highly Confidential Information, Implementer shall be liable to Philips by way of liquidated damages and not by way of penalty in an amount equal to its profits on such devices or software, and in no event less than € 500,000 (five hundred thousand Euros) or more than € 4,000,000 (four million Euros). For the purpose of this Section 9.2, any substantially related series of breaches shall be deemed a single breach. Notwithstanding the forgoing, a breach shall not be considered a Material Breach for the purposes of this Section 9.2 if Implementer maintains an internal program to assure compliance with the obligations under this Agreement and the breach was inadvertent or otherwise unintentional.

9.3 Equitable and Injunctive Relief.

The Parties agree and acknowledge that due to the unique potential for lasting effect and harm from a Material Breach of this Agreement, including the making available the means for widespread unauthorized distribution of copyrighted content intended to be protected by Vidi, if Implementer commits a Material Breach of its obligations hereunder, money damages alone may not be a sufficient remedy.

9.3.1 Equitable Relief for Philips

In case Implementer is in Material Breach of this Agreement, Philips shall be entitled, without prejudice to any other right or remedy to which Philips may be entitled hereunder, to such injunctive and other equitable relief as may be deemed proper by a court of competent jurisdiction in order to restrain such Material Breach. Any such action by Philips shall not be exclusive of any right of any Third Party Beneficiary hereunder.

9.3.2 Injunctive Relief for Eligible Content Participants

Implementer agrees that each Content Participant who at the material time is (i) a major producer of audiovisual content with an annual turnover in each of the three previous fiscal years from the production, distribution or transmission of such audiovisual content of more than one hundred million Euros and (ii) who is in compliance with its obligations under Sections 2.5 and 3.1.b of this Agreement ("Eligible Content Participant"), shall have the right to bring an action against Implementer, for any Material Breach by that is likely to result in commercially significant harm to such Eligible Content Participant, to obtain an injunction to prevent or restrain such Material Breach. The third party beneficiary right granted hereby is limited to the above referenced injunctive relief and shall not extend to monetary relief of any kind.

9.4 Third Party Beneficiary Claims.

Any Eligible Content Participant who has been or will be potentially harmed by a Material Breach by Implementer may commence an action seeking the remedies set forth in Section 9.3.2. Said Eligible Content Participants shall provide written notice to Philips within 5 business days of the commencement of said action, which notice Philips shall promptly provide to all other Content Participants. Any Eligible Content Participant who has been harmed or may be harmed by the same breach shall have the right to join in said action by seeking to intervene within 30 days of the receipt of written notice from Philips, and may not bring a separate action with respect to such breach. It is the intent of this Agreement that only one third party beneficiary action may be brought against Implementer arising out of the same breach, and this Agreement shall not be construed to create any third party beneficiary right with respect to the same breach that is not joined in the same action. Company shall not object to any motion to intervene brought in compliance with this Section 9.4. For the purpose of Sections 9.3.2 and 9.4, any substantially related series of breaches shall be deemed a single breach. Failure by a Content Participant or by Philips to provide notice hereunder shall not be a defense against any third party beneficiary claim nor shall such failure be grounds for delay in the granting of any preliminary relief.

In the event of a claim by a Eligible Content Participant brought against Implementer in accordance with the provisions of this Agreement, the prevailing party in such action shall be entitled, in addition to any form of relief as may be awarded in such action, to recover from the non-prevailing party in such action, its reasonable attorneys fees in connection with said action, provided that

Implementer shall not be responsible for attorneys fees resulting from the participation of more than one Eligible Content Participant in an action.

Eligible Content Participant shall have no right to, and Implementer and Eligible Content Participant (as the case may be) agrees that it will not, without Philips' written consent, enter into any settlement that: (i) amends any material term of any Vidi Agreement; (ii) has an adverse effect on the integrity, performance or security of Vidi with respect to operation within the Field of Use; or (iii) affects any of Philips' or HP's rights in and to Vidi or any intellectual property right embodied therein.

Nothing contained in these third party beneficiary procedures is intended to limit remedies or relief available pursuant to statutory or other claims that a third party beneficiary may have under separate legal authority.

Article 10 – Term/Termination

10.1 Termination.
This Agreement shall enter into force on the Effective Date and shall remain in force until 1 July 2014 unless terminated earlier in accordance with the provisions of this Article 10. It shall be renewed automatically for subsequent terms of 5 years, unless either party gives the other party not less than 90 days written notice prior to the end of the initial or any subsequent 5 year term, that it does not wish to renew the Agreement. Notwithstanding the foregoing Philips may terminate this Agreement forthwith by means of notice in writing to Company in the event that a creditor or other claimant takes possession of, or a receiver, administrator or similar officer is appointed over any of the assets of Company or in the event that Company makes any voluntary arrangement with its creditors or becomes subject to any court or administration order pursuant to any bankruptcy or insolvency law.

Additionally, insofar as legally permitted, Philips may terminate this Agreement at any time by means of written notice to Company in case Company or any of its Affiliates has been found liable by a competent court or administrative authority to have committed an act of willful copyright infringement for commercial gain.

10.2 Termination by Company.
Company shall have the right to terminate this Agreement at any time upon 90 days' prior written notice to Philips. Such termination, however, shall not entitle Company to a refund of any fees paid under this Agreement, nor to a waiver of fees or reporting obligations due at the time of termination. Further, any such termination shall be without prejudice to any obligations of Company at the time of such termination.

10.3 Uncured Breach.
In the event that either party materially breaches any of its obligations hereunder, and such breach is not cured within 60 days after written notice is given to the breaching party specifying the breach, then the non-breaching party may, by giving written notice thereof to the breaching party, terminate this Agreement, upon the expiration of a 60-day period beginning on the date of such notice of termination. For the purpose of this Article 10, a material breach is (a) a failure to pay any fees due

hereunder or (b) a Material Breach subject to liquidated damages under Section 9.2, or (c) failure by Company to implement reasonable measures to prevent frequent re-occurrence of revocation of Device Keys after Device Keys issued to Company have been revoked repeatedly.

10.4 Effect of Termination.
Upon expiration or early termination of this Agreement, (i) the undertaking not to assert pursuant to Section 2.1 shall no longer apply for Vidi Products and Vidi Components manufactured by Implementer after the date of expiration or termination (ii) Philips shall no longer supply any Keys to Implementer, (iii) Implementer and its Affiliates shall immediately cease the use, sale, transfer or other disposal of any such Keys, Vidi Products, and Vidi Components and within 30 days after expiration or early termination of this Agreement, Implementer shall return or destroy, in the manner directed by Philips in the Key Order Form, all Keys that are in its and in its Affiliates possession, custody or control.

10.5 Survival.
Following termination of this Agreement for any reason, the following Sections and Articles shall survive: Sections 2.4, 2.5, 4.1 (as far as related to the period before termination), 4.2, 5.1, 5.2, and 7.2, Article 8, Article 9, this Section 10.5, Article 11, Article 12, and Section 13.10.

Article 11 – Representations, Warranties, Disclaimers, and Liability Limitations

11.1 Warranties.
11.1.1 Authority to Enter into this Agreement
Philips and Company each represent and warrant (i) that it has the right, power and authority to enter into this Agreement, (ii) that the execution, delivery and performance of this Agreement have been duly authorized by it and (iii) that the person executing this Agreement on its behalf has been duly authorized to execute this Agreement and to bind the party concerned.

11.2 Disclaimer.
EXCEPT AS EXPRESSLY SET FORTH IN SECTION 11.1.1, PHILIPS MAKES NO REPRESENTATIONS OR WARRANTIES INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES (STATUTORY OR OTHERWISE), AND EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION THAT MIGHT ARISE FROM ANY ACTIVITIES OR DISCLOSURES UNDER OR RELATING TO THIS AGREEMENT. PHILIPS FURTHER DISCLAIMS ANY WARRANTY THAT THE SPECIFICATION AND ANY IMPLEMENTATION THEREOF (INCLUDING WITHOUT LIMITATION IMPLEMENTATION PROTECTION VIDI PRODUCTS AND VIDI COMPONENTS) WILL BE FREE FROM INFRINGEMENT OF ANY THIRD PARTY INTELLECTUAL PROPERTY OR PROPRIETARY RIGHTS.

11.3 Liability Limitations.
PHILIPS NOR ITS AFFILIATES, DIRECTORS, OFFICERS, AGENTS, MEMBERS, REPRESENTATIVES, EQUIVALENT CORPORATE OFFICERS, OR EMPLOYEES ACTING IN THEIR CAPACITIES AS SUCH (COLLECTIVELY, THE "AFFECTED PARTIES") SHALL BE LIABLE TO COMPANY, ITS OFFICERS, MEMBERS,

REPRESENTATIVES, AGENTS, DIRECTORS, EQUIVALENT CORPORATE OFFICIALS, AND EMPLOYEES NOR TO COMPANY'S ASSIGNEES, SUCCESSORS IN TITLE, SHAREHOLDERS, AFFILIATES, ETC. FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES ARISING OUT OF ANY CAUSE OF ACTION RELATING TO THIS AGREEMENT, OR BASED ON MAKING, USING, SELLING, OFFERING TO SELL, IMPORTING, OR DISTRIBUTING ANY PRODUCTS OF COMPANY THAT IMPLEMENT VIDI OR ANY ASPECT THEREOF, WHETHER UNDER THEORY OF CONTRACT, TORT (INCLUDING WITHOUT LIMITATION INFRINGEMENT OF INTELLECTUAL PROPERTY), INDEMNITY, PRODUCT LIABILITY, OR OTHERWISE.

IN THE EVENT THAT ANY COURT OF COMPETENT JURISDICTION RENDERS JUDGMENT AGAINST PHILIPS OR ANY AFFECTED PARTY NOTWITHSTANDING THE ABOVE LIMITATION, THE AFFECTED PARTIES' AGGREGATE LIABILITY TO COMPANY AND ITS AFFILIATES IN CONNECTION WITH THIS AGREEMENT AND WITH THE USE OF VIDI SHALL IN NO EVENT EXCEED THE AMOUNT OF MONEY PAID BY COMPANY UNDER THIS AGREEMENT FOR ANY ONE YEAR PERIOD.

Article 12 – Indemnifications

12.1 Company's Indemnification.

Company shall indemnify and hold harmless Philips and its Affiliates, HP and its Affiliates, and their respective officers, members, representatives, agents, directors, equivalent corporate officials, and employees from and against any and all damages, costs and expenses (including without limitation reasonable attorneys' fees and related expenses) which result from (i) any material breach of this Agreement, (ii) any aspect of Company's products or components, or the use thereof, other than Vidi, (iii) the use of Vidi in any manner other than as authorized by this Agreement in accordance with the Specification, (iv) the use of Vidi in any manner contrary to any provision of applicable law or (v) modifications, alterations, combinations or enhancements of Vidi not created or directed by Philips.

12.2 Philips' Indemnification.

Philips shall indemnify and hold harmless Company and its Affiliates and their respective officers, members, representatives, agents, directors, equivalent corporate officials, and employees from and against damages, costs and expenses (including without limitation reasonable attorneys' fees and related expenses) up to the amount of the limit set forth in Section 11.3, which result from the breach by Philips of any of its representations and warranties set forth in Section 11.1.1, except to the extent such claim is based upon: (i) use of Vidi other than as permitted by the Specification, (ii) modifications, alterations, combinations or enhancements of Vidi not created or directed by Philips, or (iii) any patent, copyright, trade secret or trademark that Implementer or any of its Affiliates owns (or has the right to license) and has the right to use. Notwithstanding the above, Philips' total liability under this section shall in no event exceed (i) with respect to any Company, the amount of fees paid by such Company during the immediately prior calendar year under this Agreement; or (ii) with respect to all Vidi Implementers or Content Participants within the Field of Use, the aggregate of fees received by Philips in the immediately prior calendar year under Vidi Content Protection Agreements.

Article 13 – Miscellaneous

13.1 Public Listing as Adopter

Philips shall have the right to include the name of Company in a list of adopters of the Vidi Content Protection Agreement and make such list public, unless Company notifies Philips in writing, on the Effective Date of this Agreement, that Company objects to being listed in such publication.

13.2 Ownership.

The Vidi Intellectual Property, all proprietary information in Vidi and the Specification, the media containing such Specification, and all proprietary information related to Vidi that is furnished to Company shall remain the property of Philips and HP. This Agreement grants no ownership rights to Company and, except as expressly provided herein, does not give Company any license or other right to use any of the materials or information furnished to Company hereunder.

13.3 Compliance With Export Laws.

Company acknowledges that technical data provided under this Agreement, and products based on or using these technical data, may be subject to restrictions under national export control laws. Company shall comply in full with all applicable rules and regulations on export control. Company shall obtain any approval required under such laws and regulations whenever it is necessary for export or re-export insofar as they relate to the activities under this Agreement.

13.4 Entire Agreement.

This Agreement, the Exhibits hereto and the Specification constitute the entire Agreement between Parties with respect to the subject matter hereof and supersede all prior oral, written or other agreements. Except as otherwise provided herein, this Agreement may not be modified except by written agreement dated subsequent to the date of this Agreement and signed by both Parties.

13.5 Notice.

Any notice required under this Agreement to be sent by either party shall be given in writing by letter or facsimile directed to:

a. With respect to Company, the address and contact person listed on the first page of this Agreement.

b. With respect to Philips,

Philips Intellectual Property & Standards
Legal Department
Building WAH-2
P.O. Box 220
5600 AE Eindhoven
The Netherlands

or to such other address as may have been previously specified by either party by written notice to the other party.

13.6 Assignment.
The rights granted hereunder are personal to Company, and Company's rights under this Agreement shall not be assigned or otherwise transferred except with (a) the written approval of Philips or (b) to the purchaser of all or substantially all of the outstanding capital stock or assets and obligations of Company or to the surviving entity in a merger, reorganization, or other business combination and where notice of such assignment has been provided in advance to Philips and where the surviving or acquiring company agrees in writing to be bound by this Agreement. Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the Parties, their successors and permitted assigns. Philips may assign or transfer this Agreement to any third party that agrees to assume Philips' obligations hereunder, and will provide Company with written notice thereof.

13.7 Severability.
Should any part of this Agreement judicially be declared to be invalid, unenforceable, or void by any court of competent jurisdiction, the Parties agree that the part or parts of this Agreement so held to be invalid, unenforceable, or void shall be reformed by such court without further action by the Parties hereto but only to the extent necessary to make such part or parts valid and enforceable.

13.8 No Waiver.
A waiver by either of the parties hereto of any of the covenants to be performed by the other party or any breach thereof shall not be effective unless made in writing and signed by the waiving party and shall not be construed to be a waiver of any succeeding breach thereof or of any covenant herein contained.

13.9 Most Favored Status
Philips shall offer the rights granted hereunder to all parties on fair, non-discriminatory, and equal terms. Should Philips change any provision in any other Vidi Content Protection Agreement, Company shall be given the opportunity to upgrade to such revised agreement. The benefit of any clarifications or interpretations of language shall apply to all who have executed this Vidi Content Protection Agreement. Philips shall take reasonable steps to keep Company informed of any changes to the Vidi Content Protection Agreement, clarifications, or interpretations, such as by way of example, publishing the most recent version of the Vidi Content Protection Agreement on its website.

13.10 Governing Law; Jurisdiction.
This Agreement shall be governed by and construed in accordance with the laws of the State of New York applicable to agreements made and to be performed entirely in such state. The Parties to this Agreement hereby consent to the exclusive jurisdiction and venue in the state courts located in the County of New York, New York and in the United States District Court for the Southern District of New York, except that (i) third party claims brought pursuant to Section 9.4 may be brought and adjudicated in a court sitting in Los Angeles County, California, and (ii) at the election of Philips, insofar as it and defendant(s) is concerned, the dispute may be brought and adjudicated in the competent courts in the venue of Company's registered office or in the territory where Vidi Products that do not comply with the Specifications and/or Compliance Rules are manufactured and/or sold or otherwise distributed.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the date first above written.

KONINKLIJKE PHILIPS ELECTRONICS N.V.	[COMPANY]
_____	_____
Name:	Name:
Title:	Title:
Date:	Date:

Exhibit A – Compliance and Robustness Rules

A.1 – Compliance Rules

A.1.1 Record Control Rules

A.1.1.1 Analog And Digital Inputs

Vidi is an encryption technology for video recording. This Vidi Content Protection Agreement does not itself define under what circumstances a video recording product must apply Vidi to encrypt a video recording. The rules that mandate the application of encryption technology may be set by (i) the law in the territory where a video recording product is sold, (ii) the source of the video content, and/or (iii) the format and/or patent license for the recording technology.

For example, and without limitation, rules for analog and digital inputs, that may be applicable for video recording products that use Vidi as the encryption technology, can be found in the following sources: (i) the DVD+RW Recorder Content Protection Agreement defines record control rules for the analog and digital inputs of a DVD+RW recorder, (ii) the license agreement for an Authorized Digital Output Technology (term defined in the Broadcast Flag regulation) will set the rules for encryption of video data that is received via such Authorized Digital Output Technology, (iii) the FCC defines the rules for recording video from a Broadcast Flag protected source.

A.1.1.2 Limitations On The Use Of Vidi

Vidi may be used only to encrypt video content for which the copy control information on the input indicates that (i) the Broadcast Flag is set, (ii) the EPN flag is set, or (iii) the copy control status is "Copy One Generation".

When making an encrypted recording with Vidi, the CCI and APS Trigger Bits in the Navigation Packs shall be set as follows:

- If the CCI on the input signal indicates "Copy One Generation", then CGMS bits in the Navigation Packs of the recorded audiovisual content must be set to "Copy No More" (i.e. bits 6 and 7 of Byte 80 of the Navigation Pack, as described in Section 6.4.1 of the Specification, must be set to '11').
- If the CCI on the input signal indicates "EPN" or "Broadcast Flag", then the EPN bit in Navigation Packs of the recorded audiovisual content must be set (i.e. bit 4 of Byte 80 of the Navigation Pack, as described in Section 6.4.1 of the Specification, must be set to '1').
- If so mandated by the source of the audiovisual content, the APS Trigger Bits in the Navigation Pack shall be set in accordance with the Specification.

A.1.1.3 Prevent writing Unique ID under user control

When recording the Unique ID, Data Drives and Hardware Recording Functions shall record a random, non-zero, 40-bit number as defined in Section 6.3.2 of the Specification.

Data Drives and Hardware Recording Functions shall not provide any vendor unique command, hidden command, and/or any other interface that would allow a user to specify the value of the Unique ID that is recorded.

In Data Drives and Hardware Recording Functions manufactured and shipped after July 1, 2006, a Hardware Implementation shall ensure that only random numbers can be recorded in the location that stores the Unique ID.

A.1.2 Playback Control Rules

A.1.2.1 Analog Outputs

A.1.2.1.1 Responding to the CCI and APS Trigger Bits in Navigation Packs

When playing Decrypted Audiovisual Data through an analog output, a Vidi Recorder/Player Product shall apply an analog copy protection labeling technology in compliance with the CCI and APS Trigger Bits in the Navigation Pack that is associated with this Decrypted Audiovisual Data. The applicable analog copy protection labeling technology is:

- If the APS flags in the Navigation Pack are set and the applicable CCI state is "Copy Never" or "Copy No More", then Automatic Gain Control and/or Color-stripe technologies specified in Section A.1.2.1.3 shall be applied.
- If the CGMS bits (i.e. bits 6 and 7 of Byte 80 of the Navigation Pack) are not '00', then the CGMS-A technology as specified in Section A.1.2.1.3 shall be applied.

A.1.2.1.2 Copy No More and Copy Never Content

A Vidi Recorder/Player Product shall not pass Decrypted Audiovisual Data with CCI status "Copy No More" and/or "Copy Never" to an analog output, except for (i) analog outputs for which an analog copy control labeling technologies is listed in Section A.1.2.1.3, (ii) any analog output approved for use under the DFAST License Agreement, and (iii) output to computer monitors as specified in Section A.1.2.1.5.

A.1.2.1.3 List of analog copy control labeling technologies

1. Automatic Gain Control (AGC) and color-stripe for NTSC, PAL or SECAM signals, as contained in the document titled "Specifications of the Macrovision Copy Protection Process for DVD Products, Revision 7.1.D1, September 30, 1999"
2. Automatic Gain Control (AGC) and color-stripe for 525p(480p) progressive scan signal, as contained in the document titled "Specifications of the Macrovision AGC Copy Protection Waveforms for DVD Applications with 525p (480p) Progressive scan Outputs, Revision 1.03 (December 22, 1999)"
3. CGMS-A for NTSC signals and for component (480p, 720p, 1080i) signals, as documented in:
   - IEC 61880 Video Systems (525/60) - Video and Accompanying Data Using the Vertical Blanking Interval - Analogue Interface
   - EIA/CEA-608-B Line 21 Data Services
   - CEA-805-A Data on the Component Video Interfaces
4. CGMS-A for PAL and SECAM signals, as documented in:
   - ETS 300294
   - IEC 62375

A.1.2.1.5 Computer Monitors

The Specifications do not provide the technical capability for recording high resolution video content as Encrypted Audiovisual Data. Hence, these Compliance Rules do not set constraints that

limit the output resolution of Decrypted Audiovisual Data to a computer monitor. A Vidi Recorder/Player Product may pass Decrypted Audiovisual Data through a VGA or S-VGA output to a monitor, in analog form.

A.1.2.1.6 High definition analog output

The Specifications do not provide the technical capability for recording high resolution video content as Encrypted Audiovisual Data. Hence, these Compliance Rules do not set constraints that limit the output resolution of Decrypted Audiovisual Data.

A.1.2.2 Digital Outputs

A.1.2.2.1 In the territory of the United States

In the territory of the United States, Decrypted Audiovisual Data with the state EPN shall not be transmitted on any digital output technology, except for digital output technologies that are permitted, at the time of manufacturing the Vidi Recorder/Player Product, by the FCC to be used by a "Covered Demodulator Product" for the passing of "Marked Content" pursuant to the FCC Broadcast Flag regulation (terms defined in the regulation).

In the territory of the United States, Decrypted Audiovisual Data with the state Copy No More and/or Copy Never shall not be transmitted on any digital output technology, except for digital output technologies that are approved, at the time of manufacturing the Vidi Recorder/Player Product, under the DFAST License Agreement for use in "Unidirectional Digital Cable Products" for the output of "Controlled Content" (terms defined in the DFAST License Agreement).

Notwithstanding the above, the audio portion of Decrypted Audiovisual Data with CCI status EPN or Broadcast Flag may be transferred to any analog or digital output permitted by the FCC to be used by a "Covered Demodulator Product" for the passing of the audio portion of "Marked Content" pursuant to the FCC Broadcast Flag regulation (terms defined in the regulation). The audio portion of Decrypted Audiovisual Data with CCI status Copy No More may be transferred to any analog or digital output permitted by the DFAST License Agreement for use in "Unidirectional Digital Cable Products" for the output of the audio portion of "Controlled Content" (terms defined in the DFAST License Agreement).

A.1.2.2.2 In territories with government regulation on digital output technologies

In territories where the government has regulated digital output technologies for use with terrestrial, cable, or satellite broadcast of television signals, Decrypted Audiovisual Data with the states Copy Never, Copy No More or EPN shall not be transmitted on any digital output technology except for digital output technologies approved by such government, at the time of manufacturing the Vidi Recorder/Player Product, for use in its territory.

A.1.2.2.3 In other territories

In all other territories, Decrypted Audiovisual Data shall not be transmitted on any digital output technology except for digital output technologies that are approved for use in the territory of United States under Section A.1.2.2.1.

A.1.2.4 Detection of tampering with the CCI and APS Trigger Bits in the Navigation Packs

When playing Decrypted Audiovisual Data, the Playback Function shall verify that the CCI and APS Trigger Bits in each Navigation Pack in such Decrypted Audiovisual Data are identical with the CCI and APS Trigger Bits in the CCI-MAC in said Navigation Pack, as specified in Section 6.4.1 of the Specification. If the CCI or APS Trigger Bits in said Navigation Pack is not identical with the information in the CCI-MAC, the Playback function shall select and apply the most restrictive CCI or APS Trigger Bits from Navigation Pack and CCI-MAC.

A.1.3 Integrated Products

A Playback Function may be integrated with a recording function in a single housing, provided that such recording function will not make recordings of Decrypted Audiovisual Data except for recordings that would be allowed if such recording function resided in a separate housing, and was connected with the Playback Function in compliance with Section A.1.2 of these compliance rules. Such recordings shall be subject to the same requirements for playback that they would be subject to were they made on a recording function in a separate housing.

A.1.4 Protection of the Vidi Watermarks

For the purpose of this Section A.1.4, the "Vidi Watermarks" shall comprise any of the watermark technologies selected by CableLabs in relation with the DFAST License Agreement, by Philips in relation with the DVD+RW Recorder Content Protection Agreement, by the DVD-CCA in relation with the CSS agreement, or by the DTLA in relation with its Digital Transmission License Agreement.

Commencing on the date that Philips notifies Implementer that one or more Vidi Watermarks have been identified, Implementer:
(1) Shall, when selecting among technological implementations for product features of Vidi Recorder/Player Products designed after such date, take commercially reasonable care (taking into consideration the reasonableness of the costs of implementation, as well as the comparability of their technical characteristics, of applicable commercial terms and conditions, and of their impact on audiovisual content that is encrypted or decrypted using Vidi, and on the effectiveness and visibility of the Vidi Watermarks) that Vidi Recorder/Player Products, when making an encrypted recording with Vidi or when playing back a Vidi-encrypted recording, do not strip, interfere with or obscure the Vidi Watermarks;
(2) Shall not design new Vidi Recorder/Player Products for which the primary purpose is to strip, interfere with or obscure the Vidi Watermarks when making an encrypted recording with Vidi or when playing back a Vidi-encrypted recording; and
(3) Shall not knowingly promote or knowingly advertise or knowingly cooperate in the promotion or advertising of Vidi Recorder/Player Products for the purpose of stripping, interfering with or obscuring the Vidi Watermarks when making an encrypted recording with Vidi or when playing back a Vidi-encrypted recording.

Commencing eighteen (18) months after Philips notified Implementer that one or more Vidi Watermark have been identified, Implementer:
(1) Shall not produce Vidi Recorder/Player Products for which the primary purpose is to strip, interfere with or obscure the Vidi Watermarks when making an encrypted recording with Vidi or when playing back a Vidi-encrypted recording; and

(2) Shall not knowingly distribute or knowingly cooperate in distribution of Vidi Recorder/Player Products for the purpose of stripping, interfering with or obscuring the Vidi Watermarks when making an encrypted recording with Vidi or when playing back a Vidi-encrypted recording.
(3) This Section 2.5 shall not prohibit a Vidi Recorder/Player Product from incorporating legitimate features (i.e., zooming, scaling, cropping, picture-in-picture, compression, recompression, image overlays, overlap of windows in a graphical user interface, audio mixing and equalization, video mixing and keying, down-sampling, up-sampling, and line doubling, or conversion between widely-used formats for the transport, processing and display of audiovisual signals or data, such as between analog and digital formats and between PAL, SECAM and NTSC or RGB and Y,Pb,Pr formats, as well as other features as may be added to the foregoing list from time to time by Philips by amendment to these Compliance Rules) that are not prohibited by law, and such features shall not be deemed to strip, interfere with or obscure the Vidi Watermarks when making an encrypted recording with Vidi or when playing back a Vidi-encrypted recording, provided that (a) Implementer shall, at all times after Philips identifies the Vidi Watermarks, take commercially reasonable care, in accordance with Section 2.5, that such features in a Vidi Recorder/Player Product do not strip, obscure, or interfere with the Vidi Watermark when making an encrypted recording with Vidi or when playing back a Vidi-encrypted recording, and (b) Implementer shall not knowingly market or knowingly distribute, or knowingly cooperate in marketing or distributing, such Vidi Recorder/Player Products for the purpose of stripping, obscuring or interfering with the Vidi Watermarks when making an encrypted recording with Vidi or when playing back a Vidi-encrypted recording.

A.2 – Robustness Rules

A.2.1 Construction

Vidi Recorder/Player Products as shipped shall conform to the Specifications and the Compliance Rules. Further, Vidi Recorder/Player Products shall be designed and manufactured to effectively resist attempts to modify such Vidi Recorder/Player Products to defeat the content protection system as specified by the Specifications and Compliance Rules.

A.2.2 No Defeating Functions

Vidi Recorder/Player Products shall not include:
(a) switches, buttons, jumpers, or software equivalents thereof, or
(b) traces that may be cut, or
(c) control function means (such as, but not limited to, service menus and remote-control functions),
in each case by which the provisions of the Specifications or the Compliance Rules can be defeated.

A.2.3 Robustness Methods

Vidi Recorder/Player Products shall be designed and manufactured such that they resist attempts to discover or reveal Device Keys, other Highly Confidential Information, and/or secret intermediate calculated cryptographic values used in Vidi.

Playback Functions shall not present unprotected compressed Decrypted Audiovisual Data on any user accessible bus in such a manner that permits users to circumvent or defeat the content protection system as specified by the Specifications and Compliance Rules. For these purposes, a "user accessible bus" shall mean a data bus which is designed for end user upgrades or access, such

as PCMCIA, device bay, PCI buses or Cardbus, but not memory buses, CPU buses, and similar portions of a device's internal architecture.

Software Playback Functions must make the authentication and decryption functionality tamper resistant using techniques of obfuscation to disguise its Device Keys and other Highly Confidential Information and hamper attempts to discover Highly Confidential Information. Such techniques may include for example, and without limitation: encryption, execution of a portion of the implementation in ring zero or supervisor mode, and/or embodiment in a secure physical implementation.

Software Playback Functions must perform self-checking of the integrity of its component parts and be designed to result in a failure of the implementation to provide the authorized authentication or decryption functions in the event of unauthorized modification. For these purposes, a "modification" includes any change in, or disturbance or invasion of features or characteristics, or interruption of processing, by which compressed Decrypted Audiovisual Data may be exposed to unauthorized copying, usage or distribution. Such techniques may include for example, and without limitation the use of "signed code" or other means of distributing integrity checks throughout the code.

In case the Device Keys of a Software Playback Function have been revoked because of a failure if the tamper resistance of this Software Playback Function, the tamper resistance of a new release of this Software Playback Function shall be adapted such that a repeat of this failure is resisted.

Hardware Playback Functions and Data Drives shall prevent the discovery of the Highly Confidential Information by reasonable means. Such reasonable means may include for example, without limitation, embedding the Highly Confidential Information in memory that is embedded in silicon circuitry, by encrypting the Highly Confidential Information when stored in external memory, by embedding the Highly Confidential Information in firmware which cannot reasonably be read, and/or by using the techniques described above for Software Playback Devices.

A.2.4 Required Level of Robustness

Vidi Recorder/Player Products shall be designed and implemented such that the content protection system, as specified by the Specifications and Compliance Rules, cannot be defeated or circumvented merely by an ordinary user using generally-available tools or equipment. For the purpose of this section, generally-available tools or equipment means tools or equipment that are widely available at a reasonable price, including but not limited to, screwdrivers, jumpers, clips and soldering irons. Generally-available tools or equipment also means specialized electronic tools or software tools that are widely available at a reasonable price, other than devices or technologies that are designed and made available for the specific purpose of bypassing or circumventing the protection technologies used to meet the requirements set forth in this subpart. Such specialized electronic tools or software tools includes, but is not limited to, EEPROM readers and writers, debuggers or decompilers.

A.2.5 New Circumstances

Although an implementation of a Vidi Recorder/Player Product when designed and shipped may meet the above standards, tools and equipment which were not available may become widely available at reasonable price. This availability may lead to such implementation becoming non-compliant through no act of Implementer.

Therefore, if: (a) one or more tools or equipment become generally available to users at a reasonable price, and (b) if such tools had been so available at the time of design of a particular Vidi Recorder/Player Product, such availability would have caused such products to fail to comply with these robustness rules, and (c) such availability, based on facts made known to Implementer, is likely to pose a substantial and imminent harm to Co-Implementers or Content Participants, then within eighteen (18) months after learning of a, b, and c, above, Implementer shall cease distribution of such Vidi Recorder/Player Products and shall only distribute Vidi Recorder/Player Products which are compliant with these robustness rules in view of the then current circumstances.

Exhibit B – Vidi Key Order Form (Informational)

When placing an order, please use the most recent Vidi Key Order Form, as made available to Implementer by Philips.

Name of Implementer:_____
Authorized Employee (acting as contact person regarding this transaction):
_____
E-mail Address: _____
Contact Address: _____
TEL:_____
FAX:_____

Attention of Philips:
Koninklijke Philips Electronics N.V.
Philips Intellectual Property & Standards, Licensing Support
P.O. Box 220
5600 AE Eindhoven
The Netherlands
Fax. no.: +31 40 2734131

Keys are distributed by Philips on a CD-R disc ("Distribution Disc") that contains the Keys.

Fee Schedule:

Key Fees	**Amount**
Key Fee for a Distribution Disc with Hardware Device Keys	€ 0.05 per Hardware Device Key (as defined in Section 3.3.1)
Administration Fees	**Amount**
Administration Fee for a Distribution Disc with Software Device Keys and Application Key Blocks	€ 750 per order, with a maximum of 1 distribution disc per order
Administration Fee for a Distribution Disc with DKBs	€ 750 per order, with a maximum of 100 DKBs per order
Administration Fee for a Distribution Disc with Hardware Device Keys	€ 220 per order
Shipping via DHL	order-dependent
Tax	order-dependent

Order:
Subject to the terms and conditions of the Vidi Content Protection Agreement and this Key Order Form ("KOF"), we hereby order the following Distribution Discs from Philips:

Item	**Units**	**Amount**
Distribution Disc with 32,768 Hardware Device Keys	_____ discs	x 32,768 x € 0.05 = €_____

Item	Units	Amount
Distribution Disc with 4096 Hardware Device Keys	_____ discs	x 4096 x € 0.05 = €_____
Distribution Disc with 512 Hardware Device Keys	_____ discs	x 512 x € 0.05 = €_____
Distribution Disc with Software Device Keys and Application Key Blocks (maximum 1 disc)	_____ disc	x € 750.00 = €_____
Distribution Disc with 100 DKBs (maximum 1 disc)	_____ disc	x € 750.00 = €_____
Administration Fee for a Distribution Disc with Hardware Device Keys (only if one or more distribution discs with Hardware Device Keys are ordered)		x € 220.00 = €_____
Shipping with DHL		€_____
Tax		€_____
		(Total Amount) €_____

Terms and Conditions of this order:

The capitalized terms used but not herein defined shall have the respective meanings provided in the Vidi Content Protection Agreement between Implementer and Philips (the applicable agreement being referred to as "Agreement").

1. **Order and Payment**

For Hardware Device Keys, Software Device Keys, Application Key Blocks and/or Disc Key Blocks (collectively hereinafter referred to as "Keys"), Implementer shall (i) send this KOF, signed by a duly authorized employee, by facsimile or courier to the designated Philips address, and (ii) concurrently pay the amount calculated above in the manner set forth in this KOF. Implementer confirms that this KOF shall be firm order and is not subject to cancellation after payment. In no event shall any payment made in connection with this KOF be refundable.

2. **Delivery**

Within 21 calendar days from receipt of a KOF together with the corresponding payment, Philips shall send the ordered Keys, stored on Distribution Discs, to an Authorized Employee of Implementer at Implementer's contact address. It is explicitly confirmed that Philips shall only issue the Keys after receipt of a properly completed KOF and receipt of the corresponding payment. In no event shall Philips be liable for damages caused by any delay or failure to deliver such Keys to Implementer where such failure is due to the fact that Philips has not received the order (through this KOF) or the correct payment from Implementer.

The period of 21-calender days in this Section 2 shall be increased to a period of 50 calendar days if the number of Keys ordered by Implementer (including any Keys ordered during the 30 days

preceding the day of ordering said Keys) exceeds, with a factor 2, the monthly average of the number of Keys ordered by Implementer during the preceding 3-month period.

3. **Remedy and Disclaimer**

Within 15 calendar days following the receipt of Keys from Philips, Implementer shall conduct acceptance inspection and tests in respect of the Keys received. If (i) the delivery is not in accordance with the order issued by Implementer or (ii) there is a defect in the Distribution Disc delivered by Philips to Implementer, Implementer may, within such 15 day period either (a) reject such Keys, (b) claim for replacement with new Keys, or (c) claim for repair of such Keys delivered by Philips, with proof of order and payment made by such Implementer and by returning such ordered Keys to Philips. Upon such rejection, Philips may decide at its discretion whether such rejected Keys shall be replaced or repaired. Philips EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES OTHER THAN AS PROVIDED ABOVE IN THIS ARTICLE IN RESPECT OF THE KEYS OR DISC KEY BLOCKS, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

4. **Force Majeure**

Philips shall not be considered in default or be liable for any delay or failure to perform any provisions of this KOF if such delay or failure arises directly or indirectly out of an act of nature, an act of public enemy, freight embargoes, strikes, quarantine restrictions, unusually severe weather conditions, insurrection, riot, earthquakes or any other cause or causes beyond the control of Philips.

5. **Taxes**

All costs, stamp duties, taxes and other similar levies arising from or in connection with the conclusion of this order shall be borne by Implementer. However, in the event that the government of any country imposes any income taxes on payments made by Implementer to Philips hereunder and requires Implementer to withhold such tax from such payments, Implementer may deduct such tax from such payments. In such event, Implementer shall promptly provide Philips with tax receipts issued by the relevant tax authorities so as to enable Philips to support a claim for credit against income taxes which may be payable by Philips or its Associated Companies in The Netherlands and to enable Philips to document, if necessary, its compliance with tax obligations in any jurisdiction outside The Netherlands.

6. **Payment Method**

All fees payable under this KOF shall be remitted to Philips in EURO by wire transfer to the following bank account [BANKACCOUNT], with reference [reference]

7. **Confidentiality of Keys**

Device Keys shall be treated as Highly Confidential Information under the Agreement.

8 **Use of Keys after Termination**

Without prejudice to the provisions set forth in the Agreement,
(i) Implementer shall, upon termination of the Agreement, immediately cease use of Keys;
(ii) Within 30 calendar days after termination or expiration of the Agreement, Implementer shall destroy all the remaining unused Keys, retaining no copies thereof. Implementer shall provide Philips with a written certification of such destruction signed by a senior officer of Implementer.

After termination or expiration of the Agreement, Implementer shall not attempt to retrieve or access back up information of Keys.

Agreed and Ordered by:

Signature:_____ Order Date: _____
Name of Authorized Employee:

Exhibit C – Key Fee Reporting Form

KEY FEE REPORTING FORM FOR THE VIDI CONTENT PROTECTION AGREEMENT
concluded with Koninklijke Philips Electronics N.V.

PHILIPS INTERNATIONAL B.V.
Attn. Mr. P. Speijcken
Philips Intellectual Property & Standards
GSA and Licenses Adm. Dept. (GLAD)
P.O. Box 220
5600 AE Eindhoven
The Netherlands

Date: _____
Company name: _____
Manufacturing site: _____
City: _____
Country: _____

This is to provide you with our statement under the Vidi Content Protection Agreement for the _____ quarter of the year _____.

Products	**Pieces manufactured and sold, transferred or otherwise disposed of**	**Key Fees**	**Amount due (in EUR)**
Gygis Disc (DVD+R)		**EUR 0.01**	
Gygis Disc (DVD+RW)		**EUR 0.01**	
		Total amount due:	
		Less ____ % Withholding Tax:	
		Net amount to be remitted:	

NOTE:
The (net) amount due will be paid to Philips within 60 days after the close of each calendar quarter into EUR bankaccount no. 8923019 of Koninklijke Philips Electronics N.V. - Licenses, Citibank N.A., London, swiftcode CITIGB2L, reference: "Key Fees Q... 200...".

Signed for and on behalf of ……

_____
Name:
Title:

Exhibit D – Revocation Criteria and Procedure

D.1 Revocation Criteria for Hardware Device Keys

D.1.1 A Hardware Device Key may be revoked when said Hardware Device Key is found in more than one device or product.

D.1.2. A Hardware Device Key may be revoked when said Hardware Device Key, that was issued to Implementer, was lost, stolen, intercepted or otherwise misdirected.

D.1.3. A Hardware Device Key may be revoked when Implementer has made public, sold to a third party, or disclosed said Hardware Device Key in violation of this Agreement.

D1.4. Without limiting the foregoing, a Hardware Device Key shall not be revoked (a) based on Implementer's general implementation of the Specifications in a Vidi Recorder/Player Product that is not a Compliant Vidi Product, or otherwise based on Implementer's breach of this Agreement (except that if Hardware Implementer has caused any of the circumstances described in D.1.1, D.1.2, or D.1.3, a Hardware Device Key that falls in such circumstances may be Revoked) or (b) to disable products or devices where the general security of Vidi has been compromised (other than as described in D.1.1, D.1.2, or D.1.3) by third parties.

D.2 Revocation Criteria for Software Device Keys

D.2.1 A Software Device Key may be revoked when said Software Device Key is found in one or more software application that is widely used in conjunction with the unauthorized copying and/or distribution of Decrypted Audiovisual Data

D.2.2. A Software Device Key may be revoked when said Software Device Key, that was issued to Software Implementer, was lost, stolen, intercepted or otherwise misdirected.

D.2.3. A Software Device Key may be revoked when Software Implementer has made public, sold to a third party, or disclosed said Software Device Key in violation of this Agreement.

D.2.4. A Software Device Key may be revoked when said Software Device Key, that was issued to Software Implementer, is used in a Hardware Playback Function, Hardware Recording Function, or Data Drive.

D.2.5. Without limiting the foregoing, a Software Device Key shall not be revoked (a) based on Software Implementer's general implementation of the Specifications in a Vidi Recorder/Player Product that is not a Compliant Vidi Product, or otherwise based on Software Implementer's breach of this Agreement (except that if Software Implementer has caused any of the circumstances described in D.2.1, D.2.2, D.2.3 or D.2.4, a Software Device Key that falls in such circumstances may be Revoked) or (b) to disable products or devices where the general security of Vidi has been compromised (other than as described in D.2.1, D.2.2, D.2.3 or D.2.4) by third parties.

D.3 Revocation Procedure

D.3.1 Implementer, any Co-implementer, Content Participant, Philips, and/or HP ("Requesting Party") may request Revocation of one or more Keys that were issued to Implementer ("Affected

Implementer"), and shall present Philips with written documentation of the facts that would warrant Revocation of such Keys. The documentation shall be sufficiently detailed so that Philips, or any other party, can determine solely on the basis of such documentation whether the facts averred on their face satisfy one or more of the Applicable Revocation Criteria.

D.3.2 Philips shall notify Affected Implementer of the request by Requesting Party to revoke one or more of the Keys that were issued to Affected Implementer. Affected Implementer has thirty (30) days from such notice to object to Philips in writing, explaining why the Applicable Revocation Criteria are not satisfied. If Affected Implementer does not respond or does not object, Philips shall take action to revoke the Key.

D.4.3 In the event Affected Implementer has objected within the 30-days timeframe, Affected Implementer, the Requesting Party, and Philips shall promptly meet and confer in good faith to attempt to agree whether the facts presented by Requesting Party warrant Revocation of Keys that were issued to Affected Implementer. If Affected Implementer and the Requesting Party cannot agree, the matter shall be promptly submitted to a neutral arbitrator skilled in law and the applicable technology, following the rules set out in Section D.4 and the general rules for arbitration set out in Exhibit F.

D.4 Rules for Arbitration

D.4.1 Any disagreement between Affected Implementer and Requesting Party, shall be settled by arbitration administered by the American Arbitration Association in accordance with its Commercial Arbitration Rules including its Supplementary Procedures for online Arbitration (as published by the American Arbitration Association on its website http://www.adr.org/), and judgment on the award rendered by the arbitrator(s) may be entered in any court having jurisdiction thereof.

D.4.2 The parties to the arbitration shall be the Requesting Party, and the Affected Implementer (collectively, the "Arbitration Parties"). The Requesting Party shall bear the burden of proof in demonstrating, by a preponderance of the evidence, that one or more of the Applicable Revocation Criteria have been satisfied.

D.4.3 The arbitrator(s) is (are) empowered solely to determine whether one or more of the applicable revocation criteria have been satisfied. In the event that the arbitrator(s) determine(s) that the Applicable Revocation Criteria set forth in Exhibit D of this Agreement have been satisfied, Revocation shall be deemed warranted.

D.4.4 The prevailing party in such arbitration shall provide Philips with a copy of the arbitrator(s) decision. If, pursuant to Section D.4.3, Revocation is warranted, Philips shall, after it receives such decision, take action to cause such Revocation.

Exhibit E – Acknowledgement Form for Authorized Employees

I,_____, a full-time regular employee of _____("Implementer"), acknowledge that I have been designated by Implementer as an "Authorized Employee" to receive, on behalf of Implementer, access to Highly Confidential Information of Koninklijke Philips Electronics N.V which Implementer is obliged to maintain strictly confidential under the terms of the Vidi Content Protection Agreement between Koninklijke Philips Electronics N.V and Implementer.

I further acknowledge that the Vidi Content Protection Agreement requires Implementer to employ procedures for safeguarding Highly Confidential Information.

Such procedures employed by Implementer for safeguarding Highly Confidential Information shall be at least as rigorous as Implementer would employ for its own most highly confidential information,. Such procedures shall include, at a minimum:

(1) Implementer shall maintain on its premises a secure location in which any and all Highly Confidential Information shall be stored;
(2) any Highly Confidential Information stored in such a location shall be accessible only by Authorized Employees;
(3) Implementer shall keep a record of access of the Highly Confidential Information by Authorized Employees; and
(4) as long as Highly Confidential Information is not in use, such information shall be stored in a locked safe at such secure location.

I further acknowledge that the Vidi Content Protection Agreement defines Device Keys as Highly Confidential Information.

I further acknowledge that I have signed a prior written agreement with Implementer pursuant to which I have agreed to maintain the confidentiality of third party confidential information received by Implementer. I acknowledge that I am bound by such agreement to adhere to procedures established by Implementer to maintain the confidential nature of Confidential Information and Highly Confidential Information during my employment and at least two years after the termination of my employment with Implementer.

By signing below, I attest that I have read and understood this acknowledgement and accept to be bound by its terms.

Signed: _____

Name: _____

Date: _____

Email: _____

Address: _____

Copy to: Philips International B.V.
Philips Intellectual Property & Standards
Legal Department
Building WAH-2
P.O. Box 220
5600 AE Eindhoven
The Netherlands

Exhibit F – General Rules for Arbitration

F.1 The language of the arbitration shall be English.

F.2 The place of arbitration shall be New York, New York, U.S.A.

F.3 The dispute shall be submitted to three neutral arbitrators selected from a group of persons with knowledge of, and experience in, the technology, the various industries, and the law.

F.4 The arbitrators may conduct the arbitration in such manner as they shall deem appropriate, including the imposition of time limits that they considers reasonable for each phase of the proceeding, but with due regard for the need to act, and make a final determination, in an expeditious manner. The arbitrators shall set a schedule to endeavor to complete the arbitration within 60 days.

F.5 The arbitrators shall permit and facilitate such limited discovery as they shall determine is reasonably necessary, taking into account the needs of the Arbitrating Parties and the desirability of making discovery as expeditious and cost-effective as possible, recognizing the need to discover relevant information and that only one party may have such information.

F.6 The Arbitrating Parties and the arbitrators shall treat the arbitration proceedings, any related discovery, documents and other evidence submitted to the arbitrators as Confidential Information, and as necessary, the arbitrators may issue orders to protect the confidentiality of proprietary information, trade secrets and other sensitive information disclosed in discovery or otherwise during the arbitration. Except as may be required by law, neither an Arbitrating Party nor an arbitrator may disclose the existence, content, or results of any arbitration hereunder without the prior written consent of both parties.

F.7 Any decision by the arbitrators shall be final and binding on the Arbitrating Parties and Philips, except that whether the arbitrators exceeded their authority, as specifically described in this Agreement, shall be fully reviewable by a court of competent jurisdiction.

F.8 The arbitrators may determine how the costs and expenses of the arbitration shall be allocated between the Arbitrating Parties, but they shall not award attorneys' fees, provided that in the event that one of the Arbitrating Parties, in the opinion of the arbitrators, initiated the arbitration procedure frivolously, the arbitrators may decide to award attorneys' fees to the other party.

Exhibit G – Table of Contents (Informational)